Arctic RTU User's Manual

Arctic RTU (2910, 2920, 2930)

Firmware Version 5.2.x
Document Version 1.1
November 2014

Copyright and Trademark

Copyright © 2008-2014, Viola Systems Ltd. All rights to this manual are owned solely by Viola Systems Ltd. (referred elsewhere in this User's Manual as Viola Systems). All rights reserved. No part of this manual may be transmitted or reproduced in any form or by any means without a prior written permission from Viola Systems.

Ethernet™ is a trademark of XEROX Corporation. Windows™ and Internet Explorer™ are trademarks of Microsoft Corporation. Netscape™ is a trademark of Netscape Communications Corporation. All other product names mentioned in this manual are the property of their respective owners, whose rights regarding the trademarks are acknowledged.

Viola Systems Ltd.

Lemminkäisenkatu 14-18 B

FI-20520 Turku

Finland

E-mail: info@violasystems.com

Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: http://www.violasystems.com

Disclaimer

Viola Systems reserves the right to change the technical specifications or functions of its products or to discontinue the manufacture of any of its products or to discontinue the support of any of its products without any written announcement and urges its customers to ensure that the information at their disposal is valid.

Viola software and programs are delivered “as is”. The manufacturer does not grant any kind of warranty including guarantees on suitability and applicability to a certain application. Under no circumstance is the manufacturer or the developer of a program responsible for any damage possibly caused by the use of a program. The names of the programs as well as all copyrights relating to the programs are the sole property of Viola Systems. Any transfer, licensing to a third party, leasing, renting, transportation, copying, editing, translating, modifying into another programming language or reverse engineering for any intent is forbidden without the written consent of Viola Systems.

Viola Systems has attempted to verify that the information in this manual is correct with regard to the state of products and software on the publication date of the manual. We assume no responsibility for possible errors which may appear in this manual. Information in this manual may change without prior notice from Viola Systems.

Declaration of Conformity

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name: Viola Systems Ltd.

Manufacturer's Address:

Lemminkäisenkatu 14-18 B

FI-20520 Turku

Finland

declares that this product:

Product Name:

Arctic RTU

conforms to the following standards:

EMC:

EN 55022 Emission Test (Class A)

1. Radiated Emissions (30-1000MHz)
2. Conducted Emissions (0.15-30MHz)

EN 50082-1 Immunity Test

1. IEC 801-3: Radio Frequency Electromagnetic Field
2. IEC 801-2: Electrostatic Discharge
3. IEC 801-4: Fast Transients, AC Power Ports and Signal cables

Supplementary Information:

"The product complies with the requirements of the Low Voltage Directive 73/23/EEC and EMC directive 89/336/EEC."

Note!
This is a Class A product. In a domestic environment this product may cause radio Interference which may make it necessary for the user to take adequate measures.

Manufacturer's Contact Information:

Viola Systems Ltd.

Lemminkäisenkatu 14-18 B

FI-20520 Turku

Finland

Phone: +358 20 1226 226

Fax: +358 20 1226 220

Warranty and Safety Instructions

Read these safety instructions carefully before using the products mentioned in this manual:

Warranty will be void if the product is used in any way in contradiction with the instructions given in this manual or if the product has been tampered with.

The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the devices is appropriate. This also applies to the maintenance of the products.

To prevent damage both the product and any terminal devices must always be switched OFF before connecting or disconnecting any cables. It should be ascertained that different devices used have the same ground potential. Before connecting any power cables the output voltage of the power supply should be checked.

This product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment or as part of such equipment in any hazardous environment requiring fail- safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of Viola Systems manufactured hardware or software could lead directly to death, personal injury, or severe physical or environmental damage.

Revisions

Date	Document Version	Firmware Version	Description of Changes
03/2013	1.0	-	First version
11/2014	1.1	-	Minor text changes

Contents

COPYRIGHT AND TRADEMARK 2
DISCLAIMER 3
DECLARATION OF CONFORMITY 4
WARRANTY AND SAFETY INSTRUCTIONS 5
REVISIONS 6
1. INTRODUCTION 9
1.1 About this User's Manual 9
1.2 The Arctic Platform 10
2. PHYSICAL INTERFACES 12
2.1 Front Panel Description 12
2.2 Back Panel Description 13
2.3 Side Panel Description 14
2.4 Product Information Label 15
2.5 Firmware Version 16
3. GETTING STARTED 17
3.1 Installation of the Arctic 17
3.2 Setting the IP address in web browser 17
3.3 Setting the IP address in console 19
4. ARCTIC CONFIGURATOR TOOL 22
4.1 Login to Arctic Configurator 22
4.2 General Usage of the Arctic Configurator 23
5. WIRELESS CONNECTION 24
5.1 Antenna 24
5.2 SIM Card and Card Holder 24
5.3 Configuring Arctic's GPRS Settings 24
5.4 Useful GSM/GPRS Information 26
6. ARCTIC SOFTWARE CONFIGURATION 27
6.1 System Menu 27
6.2 Network Menu 27
6.2.1 Ethernet LAN 28
6.2.2 GPRS 28
6.2.3 Dial-in 29
6.2.4 SSH-VPN 29
6.2.5 L2TP-VPN 31
6.2.6 GRE 32
6.2.7 Monitor 33
6.2.8 Routing 34
6.2.9 S-NAT 34
6.2.10 D-NAT 34
6.2.11 DNS Update 35
6.2.12 DynDNS Client 35
6.2.13 NTP Client 36
6.2.14 SMS Config 37

6.3 Firewall Menu....37
6.4 Service Menu....39
6.4.1 Web Server....39
6.4.2 SSH....39
6.4.3 Telnet....39
6.4.4 DHCP....39
6.5 Application Menu....41
6.6 Tools Menu....41

7. I/O INTERFACE....43
7.1 Digital Input (IO-1)....43
7.2 Digital Output (IO-1)....44
7.3 DC Output....44
7.4 IO-2 connector....44
7.4.1 Digital Input (IO-2)....45
7.4.2 Digital Output (IO-2)....45
7.4.3 Analog Input (IO-2)....45

8. MODBUS APPLICATION SETTINGS....46
8.1 Introduction....46
8.2 Parameters....46
8.2.1 Common parameters....46
8.2.2 Routes....52
8.2.3 Saving Parameters....54
8.3 Configuring Network Master to Serial Slaves Mode....54
8.3.1 Settings – Common parameters....55
8.3.2 Saving Parameters....57
8.4 Configuring Serial Master to Network Slaves Mode....58
8.4.1 Settings – Common Parameters....58
8.4.2 Settings – Routes....60
8.4.3 Making Settings Permanent....62
8.5 Modbus I/O settings....62

9. IEC-104 APPLICATION SETTINGS....64
9.1 General settings....64
9.2 Serial settings....65
9.3 Network settings....66
9.4 IEC-104 Settings....68
9.5 IEC-101 settings....71
9.6 ASDU Converter....74
9.7 Packet collector....75
9.8 Other settings....77
9.9 IEC-104 I/O settings....77

10.TROUBLESHOOTING....79
10.1 Common Problems....79

SPECIFICATIONS....80

LIMITED WARRANTY....81

TECHNICAL SUPPORT....82

1 Introduction

The Arctic RTU product family includes a number of Arctic RTU product variants. Arctic RTU products provide wireless monitoring and control of field devices via commercial mobile network connectivity to central control systems like SCADA. Several interfaces are available for field device connectivity: Digital inputs and outputs, analog inputs, serial and Ethernet ports. Industrial protocols IEC-104 and ModbusTCP are supported for SCADA connectivity. With Arctic RTU protocol conversion feature the conventional IEC-101 and Modbus serial devices can be connected in a reliable way to a modern TCP/IP based IEC-104 and Modbus TCP control systems via GPRS and EDGE mobile networks.

1.1 About this User's Manual

This User's Manual describes the operation of the Arctic RTU. All devices in this User's Manual are referred to as Arctic, unless otherwise mentioned. This manual provides introductory information as well as detailed instructions on how to set up and manage the Arctic as part of a network environment. It is intended for anyone involved in installing and managing Arctic devices. It is assumed that the reader of this manual is familiar with basic working principles of Internet technology.

There are three Arctic RTU product variants. They have the following features:

Table 1: Arctic RTU product variants comparison

Feature	2910 / Arctic RTU (Modbus, IO-1)	2920 / Arctic RTU (IEC-104, IO-1)	2930 / Arctic RTU (IEC-104, EDGE, IO-2)
GPRS	yes	yes	yes
EDGE	no	no	yes
6-26 V_{DC} input voltage	yes	yes	no
8-48 V_{DC} input voltage	no	no	yes
IEC-101 to IEC-104 protocol conversion	no	yes	yes
Modbus ASCII/RTU to Modbus TCP protocol conversion	yes	no	no
Analog input (4-20 mA)	none	none	2
Digital inputs	8	8	6
Digital outputs	2	2	4

Figure 1. *Arctic RTU (2910 and 2920)*

Figure 2. *Arctic RTU (2930)*

1.2 The Arctic Platform

The Arctic platform utilizes a number of wireless or fixed line interfaces depending on your specific requirements. Arctic is a customizable technology allowing users to develop solutions for their own applications. Arctic devices

have been designed to withstand the requirements of extreme environments and industrial use.

Technical Features Summary

The following are the functional components in the Arctic RTU device.

Details of the each components are listed below:

HARDWARE

CPU Platform:

- 32-bit RISC microcontroller
- 32 MB RAM
- 8 MB Solid state FLASH memory

Network Interface:

- 10/100 Base-T Ethernet (RJ45)

Device Interface:

- 2 Serial ports (RS-232, RS-485)
- I/O connector

Mechanics:

- Aluminum frame
- Attachment rail for optional and custom mounting tools

SOFTWARE

Operating System:

- Linux

Supported Protocols:

- PPP, IP, ICMP, UDP, TCP, ARP, DNS, DHCP, FTP, TFTP, HTTP

Application Services:

- HTTP server, CGI
- FTP client
- SSH server and client
- OpenVPN
- IPsec
- Temperature sensor
- Real Time Clock
- Syslog
- DHCP server and client
- Status querying using SMS
- Serial connection (Serial GW)

Management and Configuration:

- Web user interface
- Console port

2 Physical Interfaces

The Arctic unit contains three panels for interface connections and status indication. These panels are:

2.1 Front Panel Description

The front panel of the Arctic consists of the following connectors and switches:

Figure 3. *Front Panel (2910 and 2920)*

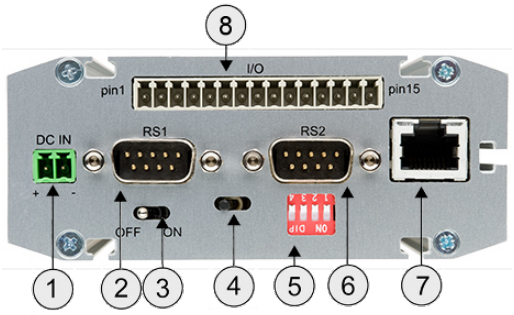
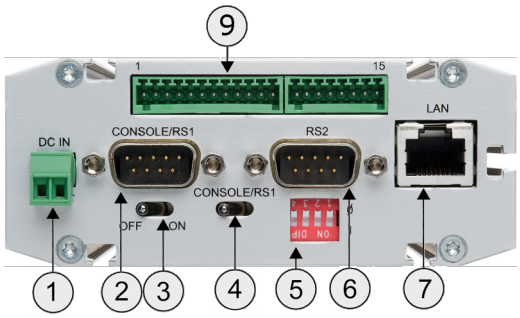


Figure 4. *Front Panel (2930)*



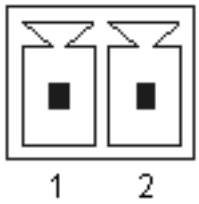
1. Power supply connector
2. Application/console serial port (RS1)
3. Power switch
4. Console switch
5. DIP switches
6. Application serial port (RS2)
7. Ethernet connector
8. *IO-1* (2910, 2920), digital I/O connector
9. *IO-2* (2930), digital & analog I/O connector

The Arctic has rails to enable wall or DIN rail mounting. The front panel contains slots for nuts or other mounting accessories (optional) in order to gain access to these rails.

Power Supply Connector

The Arctic has a VDC power supply connector as shown in the figure below.

Figure 5. *Power supply connector*



- Pin 1 is positive (+)
- Pin 2 is negative (–)

The unit is protected against reversed polarity.

Power Switch

Enables or disables the operation of the Arctic.

Ethernet Connector

Arctic has an RJ45 connector for 10/100 Mbps Ethernet connection. Maximum length of the Ethernet cable is 100m.

The figure and pin description of the Arctic's RJ45 Ethernet connector is as follows:

Figure 6. *RJ45 Ethernet connector*

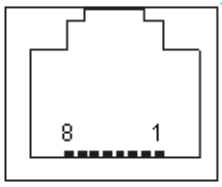


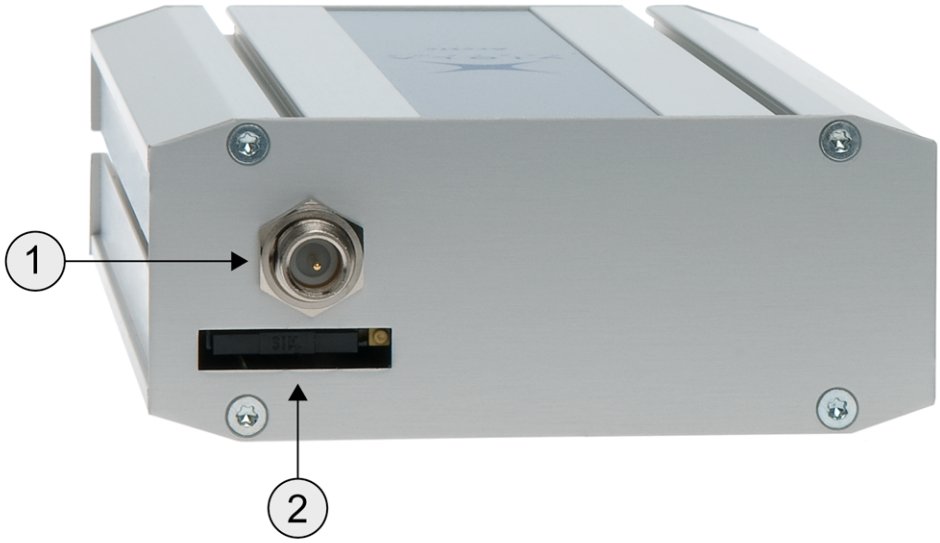
Table 2: RJ45 Ethernet connector PIN Description

Pin Number	Name	Direction	Explanation
1	Rx+	IN	Data Receive Positive
2	Rx–	IN	Data Receive Negative
3	Tx+	OUT	Data Transmit Positive
4	NC	-	-
5	NC	-	-
6	Tx–	OUT	Data Transmit Negative
7	NC	-	-
8	NC	-	-

2.2 Back Panel Description

The Arctic has an antenna connector and a slot for a SIM card on the back panel.

Figure 7. *Back Panel*



1. FME connector for an antenna.
2. SIM Card slot.

2.3 Side Panel Description

The side panel of the device contains ten LEDs which are used to indicate the status of the Arctic and only five of them are connected. The LEDs are numbered from 1 to 10 starting from the rear panel side. A detailed description of each LED is listed below:

Figure 8. *LED Description*

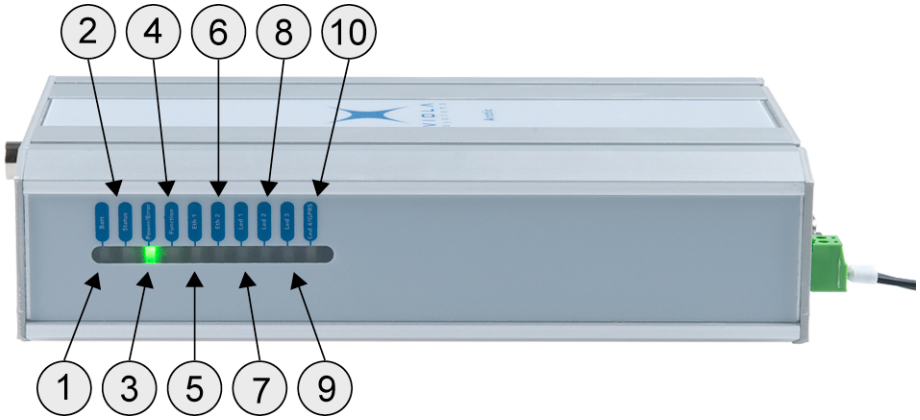


Table 3: LED Description

LED Number	LED	State	Description
1	Battery		Not connected
2	VPN	ON	VPN connection is up

LED Number	LED	State	Description
		Blinking	VPN onnection is starting
		OFF	VPN connection is disabled
3	Power/Error	ON	Operating power is turned on
		OFF	Operating power is turned off
4	System Function	ON	Device is starting
		Blinking	Device is operating normally
5	Eth 1	ON	Ethernet link is up
		Blinking	Ethernet link is transferring data
		OFF	Ethernet link is down
6	Eth 2		Not connected
7	LED 1		Not connected
8	LED 2		Not connected
9	LED 3		Not connected
10	LED 4/GPRS	Blinking	Wireless communication is starting or transferring data
		OFF	Wireless communication is inactive

2.4 Product Information Label

The product information label on the underside of the Arctic contains the following information:

1. Product type
2. Serial number
3. MAC address

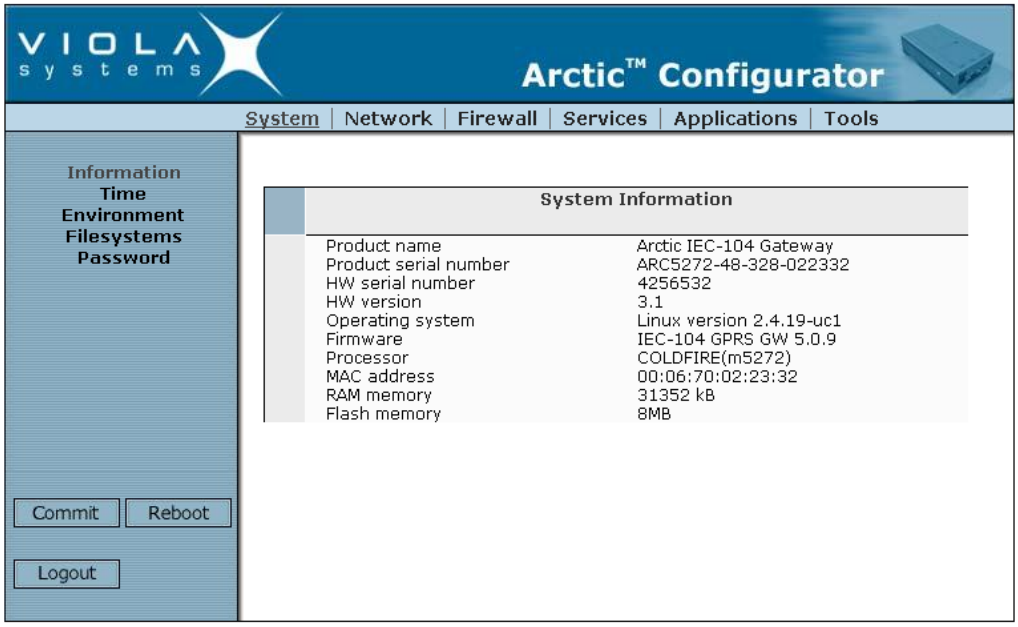
   The Ethernet address (MAC address) of the unit is printed on the product label. Each address code starts with the digits “00:06:70”, but the remaining six digits are unique for each unit.

Figure 9. *Product Information Label*

2.5 Firmware Version

The Arctic firmware version may be checked from the Viola Configurator startup page (System -> Information). It is also possible to get the firmware version by issuing command *firmware* in console.

Figure 10. *Firmware Version*



This manual describes the series 5 firmware version RTU 5.2.x.

3 Getting Started

3.1 Installation of the Arctic

When installing Arctic models with wireless connectivity options, it should be remembered that high-frequency radio waves need to be taken into account. The surrounding environment affects the range of radio signals. Therefore, if you are using an Arctic with antennas directly mounted to the antenna connector, try to avoid placing the Arctic where the radio signal might be disturbed (“shadowed”) by nearby obstacles. Also large metallic surfaces (racks) may have a highly detrimental effect on the antenna performance. In case of metal racks or surfaces, it is recommended to use an external antenna with an appropriately selected cable. By following these precautions, the Arctic may be installed more freely.

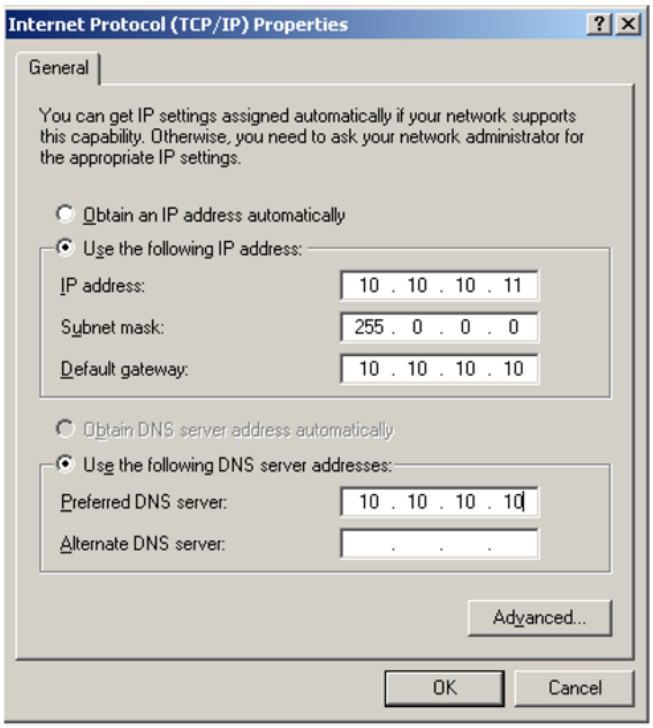
The aluminum case of the Arctic contains rails for wall or DIN rain mounting. Both broad sides contain two rails and the narrow side opposite to the LED panel contains one rail. These rails allow a flexible selection of the optimum mounting direction. A mounting kit for DIN rail mounting is available as an accessory.

3.2 Setting the IP address in web browser

This is the recommendable way to set up the network parameters. It is an easy-to-apply solution if the computer used for configuration has been properly configured. Follow the procedure listed below:

1. Connect to the Arctic using your HTML browser. The default IP address of the Arctic is “10.10.10.10” (netmask “255.0.0.0”). Computer connected to Viola Arctic device can use for example IP address 10.10.10.11.

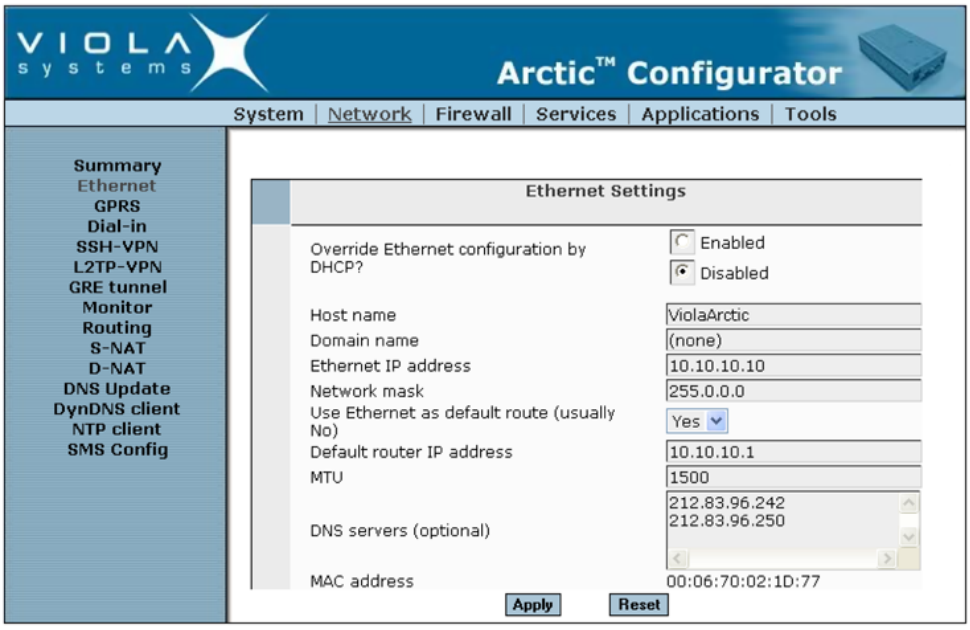
Figure 11. *IP Properties*


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 10 . 10 . 11
Subnet mask:
255 . 0 . 0 . 0
Default gateway:
10 . 10 . 10 . 10
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
10 . 10 . 10 . 10
Alternate DNS server:
Advanced...
OK
Cancel

2. From the initial page, click **Start Configurator** and enter login information in the following page. Username is *root* and by default no password is set (just leave the field empty).

3. Navigate to Network -> Ethernet page.

Figure 12. *Ethernet Settings*



4. Enter the Ethernet IP address (and other network settings) of your choice and click Apply and then Commit (on bottom of page) to store the settings.
5. Reboot the Arctic for the settings to take effect.

Note!
Arctic default password is *empty*. Remember to set the password before connecting the Arctic device to a public network.

3.3 Setting the IP address in console

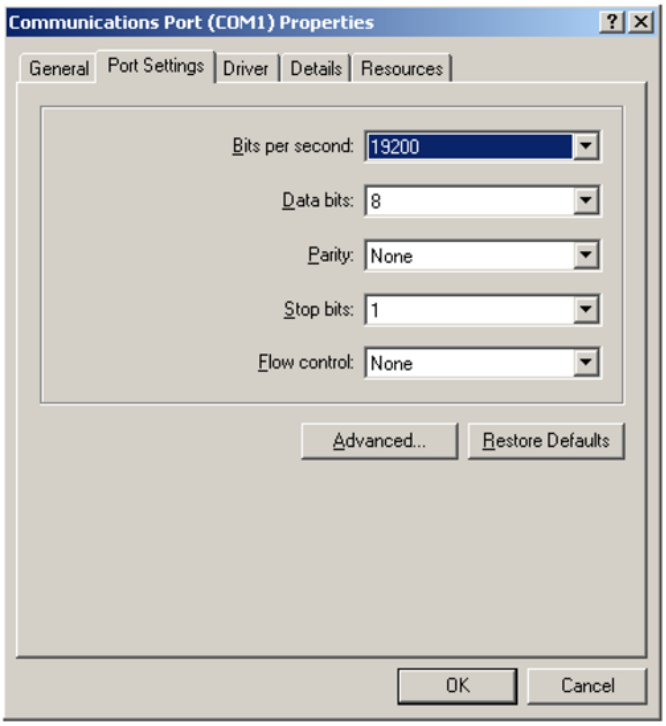
Before installation, you need to find out the required network settings. These include the **IP Address**, **Netmask** and **Gateway Settings** used by the Arctic. The local network administrator can provide them to you or you can ask for them from your Internet Service Provider.

Note!
If possible, it is recommended to use an HTML browser to set up network settings as described in the next chapter. If using a console, please follow the procedure below:

1. Before you start, turn off the power from all devices and check that the power switch of the Arctic is in the “OFF” position.
2. Connect a serial cable (crossover) to the console serial port (RS1) and an Ethernet cable to the RJ45 connector.
3. Switch the Arctic on by toggling the power switch to “ON” position.

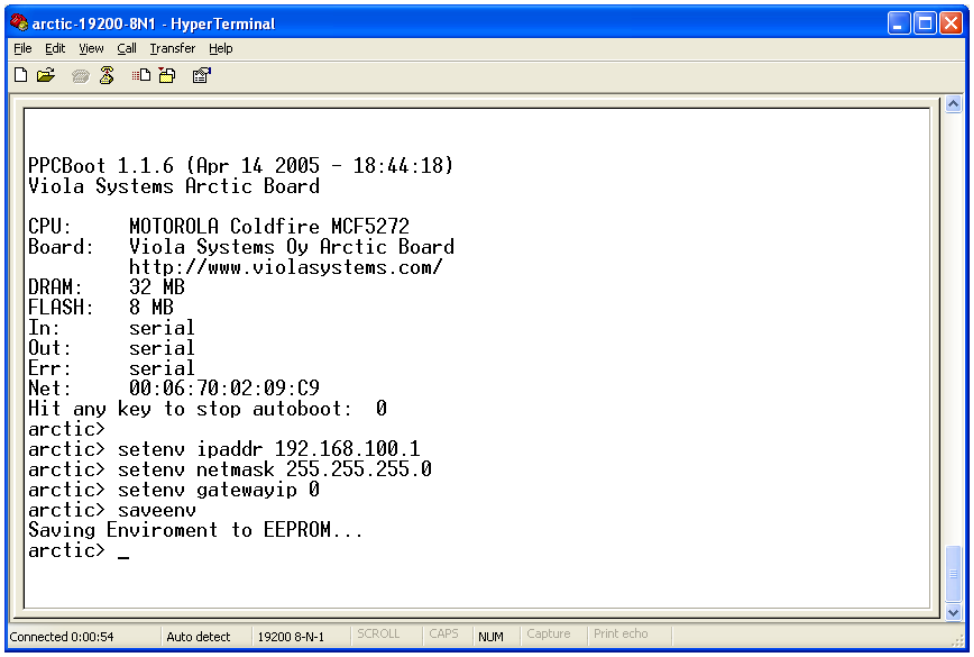
4. Connect to Arctic using COM port and terminal program (Hyperterminal). Serial settings for console (RS1) are 19200-8-N-1 and "Flow control set to none".

Figure 13. *COM1 Properties*



5. Stop the PPCboot to get the “Arctic>” command prompt. Set the IP address and netmask using command “setenv”.

Figure 14. *Arctic COM1 Hyperterminal*



6. Save the setting with command “saveenv”.
7. Reboot the Arctic for the settings to take effect.

Note!
Default gateway value (gatewayip) is usually set to zero (0) because GPRS or VPN is used as default router.

4 Arctic Configurator Tool

The Arctic Configurator is a tool which allows the user to manage the properties of the Arctic device by using a user-friendly, www-based interface. You only need a computer with an HTML browser and a working connection to the Arctic to be able to use the web configurator.

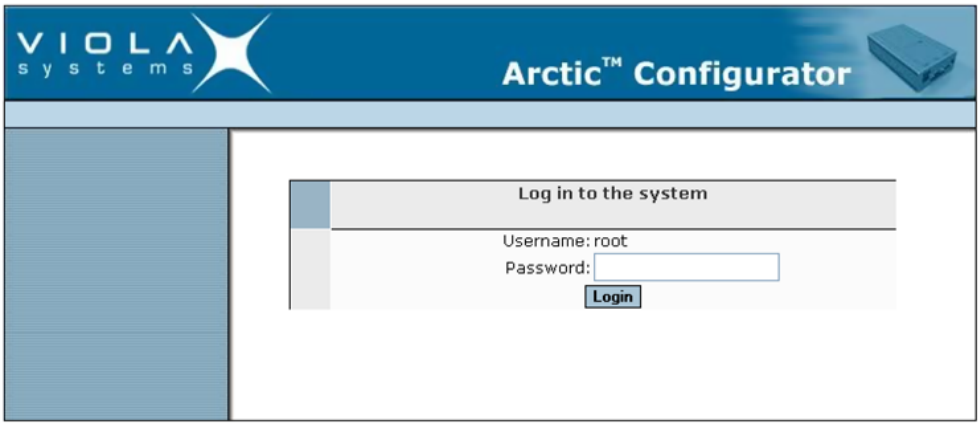
With the Arctic Configurator, you can set important parameters, receive status information, and set variables that control which applications and processes run on the Arctic board.

4.1 Login to Arctic Configurator

To start using the Arctic Configurator, open the URL where the Arctic is located and it has to be configured. On the Viola Arctic main page, select the **Start Configurator** link.

Figure 15. *Start Configurator*

Figure 16. *System Log-in*



Initially, the Arctic Configurator will ask you for the password for the Arctic device root-account. Enter the correct password in the box provided and press the login-button to start the Arctic Configurator.

Note!
Default password for root is empty. Remember to set the password before connecting the device to a public network.Password can be changed from System -> Password menu.

4.2 General Usage of the Arctic Configurator

After a successful login, the Arctic Configurator will display the main screen. This consists of the main navigation menu on the top, the secondary navigation bar on the left, and the main screen containing the currently active content and controls.

When the program starts for the first time, the System/Information screen will be shown in the main content area. The main navigation-menu on the top of the screen is used to navigate between the different subsets of settings available. Selecting an item from the main menu will display the available items related to this subset in the secondary navigation bar, selecting the first of these to be shown in the main content area.

The secondary navigation-bar on the left contains the groups of parameters in this subset. Selecting an item from this menu will display the content related to the selected group in the main content area. In the bottom of the secondary navigation-bar is a group of three buttons which are always visible: **Commit**, **Reboot** and **Logout**. The Commit-button is used to save the memory-resident data for "soft" parameters permanently to non-volatile memory. Note that the values for the previous parameters are not saved to non-volatile memory unless the Commit-button is pressed. The Reboot-button, as the name suggests, will reboot the Arctic. The Logout button will end the current session and return to the login-screen.

5 Wireless Connection

5.1 Antenna

The Arctic has a FME connector (male type) for an external antenna. It is possible to use any kind of external 50 Ω dual-band antenna intended for GSM900 (880–960 MHz) and GSM1800 (1710–1880 MHz) frequency bands. Connect the antenna directly to the connector provided for the antenna on the back panel of the Arctic unit.

Typically, commercially available antennas are provided with a flexible 50Ω cable having a length of 2–3 meters and having a female type FME-connector.

Different kinds of Viola antennas are available as accessories. See the figure below.

Figure 17. *Rooflex Puck Antenna*

5.2 SIM Card and Card Holder

Standard 3 V SIM cards may be used with the Arctic RTU. A SIM card holder is located on the back panel near the GPRS antenna connector. If you have the PIN code query enabled, check that the Arctic Configurator has a correct PIN code entered in the GPRS submenu. To operate with SIM card follow the procedure below:

Note!
Do **not** insert or remove the SIM card while the GPRS module is in operation. The SIM card contents may become corrupted if the card is removed while the GPRS module is writing data to it.

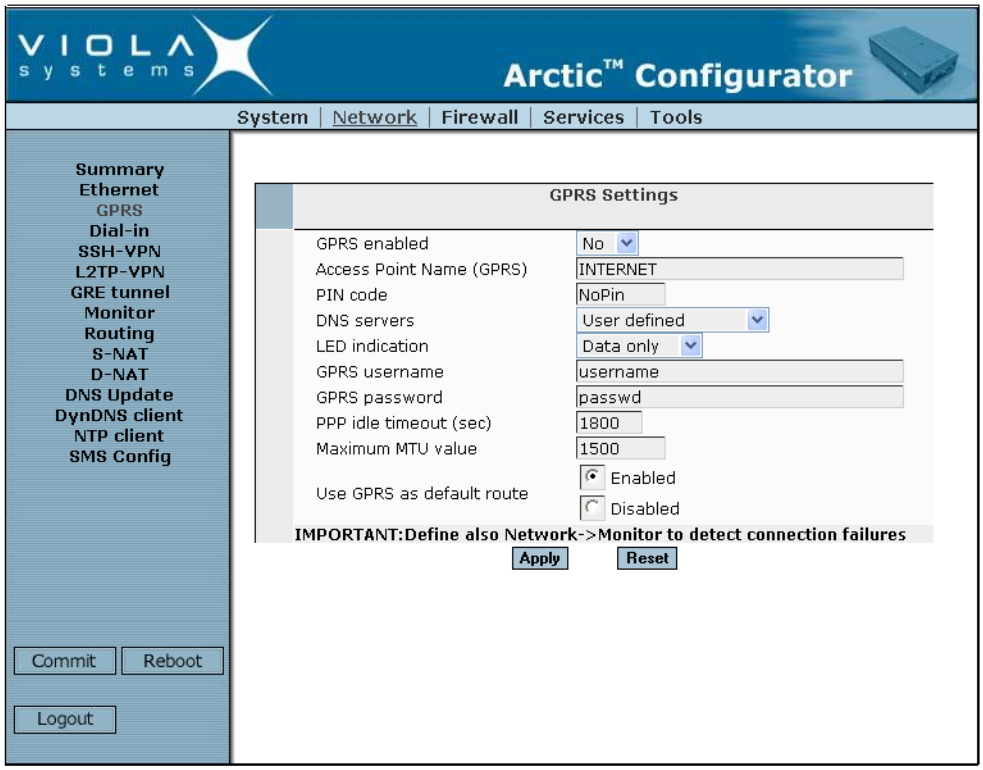
1. Power off the Arctic.
2. The SIM card holder contains a tray with a yellow eject button. Push this button in order to eject the tray from the holder.
3. Put the SIM card onto the tray.
4. Insert the tray carefully back to the holder and press the tray until it is locked.

5.3 Configuring Arctic's GPRS Settings

1. If your SIM card has the PIN code querying set, make sure you **configure the PIN code before inserting the card in the card holder**. If PIN querying is not set, you may proceed with the card installation procedure.
2. Connect to the Arctic and log in to Configurator.

3. Navigate to Network page from main navigation bar and select the GPRS sub page.
4. Set the access point name appropriately (usually “INTERNET”) .
5. Set the GPRS network username and password appropriately if your GPRS service requires authentication.
6. Set default route to *enabled*.
7. Optionally, set the PIN code and PPP idle timeout.
   - If your SIM card has the PIN code set, type the code into the PIN code field.
   - PPP idle timeout defines the time in seconds how often the Arctic resets the GPRS connection if the connection is idle.
   - ICMP Echo is used to monitor GPRS connection between Arctic and a remote host. If the designated host cannot be reached the GPRS connection is reset. This feature should be always enabled from Network -> Monitor menu.
8. Finally click on **Apply**, wait for the confirmation and then click on **commit** to store the settings. Again, wait for **commit** confirmation.

Figure 18. *GPRS Settings*



Reboot the Arctic for the settings to take effect. Check GPRS status from Network/Summary Menu.

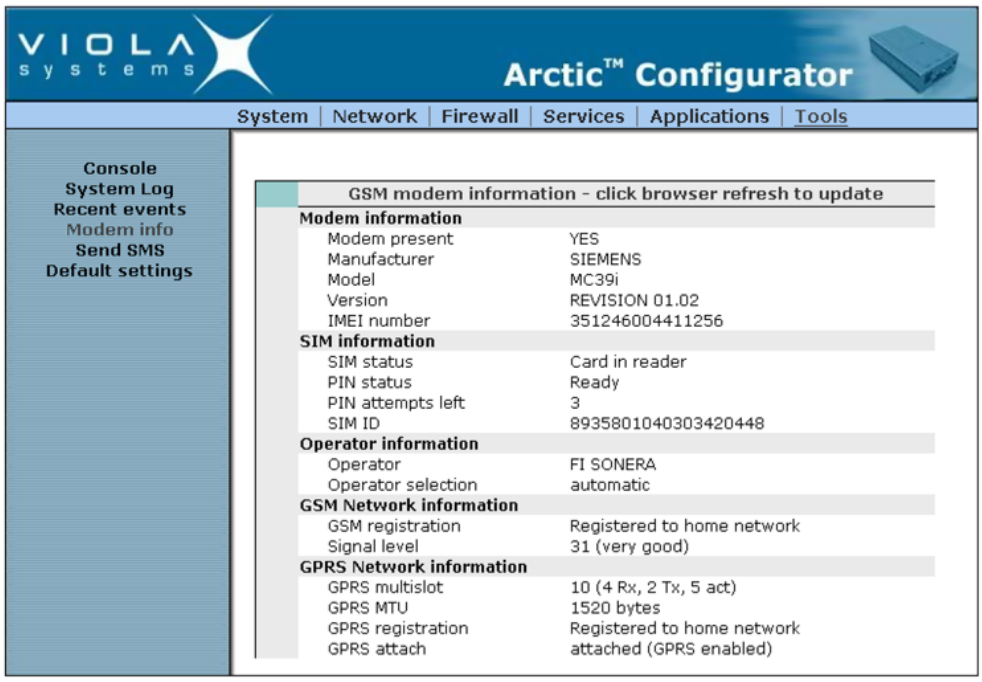
Note!

It is important to set the correct PIN code with the Arctic Configurator before plugging the SIM card in. If an incorrect PIN is set and the PIN is required by the SIM card, the Arctic will not retry with the wrong PIN, thus avoiding the SIM card lock-up. In such a case, you will need to insert the SIM card to a mobile phone and enter the correct PIN before continuing.

5.4 Useful GSM/GPRS Information

Useful GSM/GPRS information can be obtained from Tool -> Modem Info Menu.

Figure 19. *Useful GSM/GPRS Information*



6 Arctic Software Configuration

6.1 System Menu

The System-menu contains items that are relevant to the Arctic board itself. It allows the user to view information about the system or the current executing environment and to set the date and time.

Information – submenu contains general information about the Arctic device. Information on this submenu should be provided if possible when contacting Viola Systems technical support.

Time – submenu contains time information. Arctic has a real time clock with battery backup and time information may be adjusted here.

Note!
Updated time data is not saved permanently until the **Commit** button is pressed. Until then, it will be stored only in RAM memory.

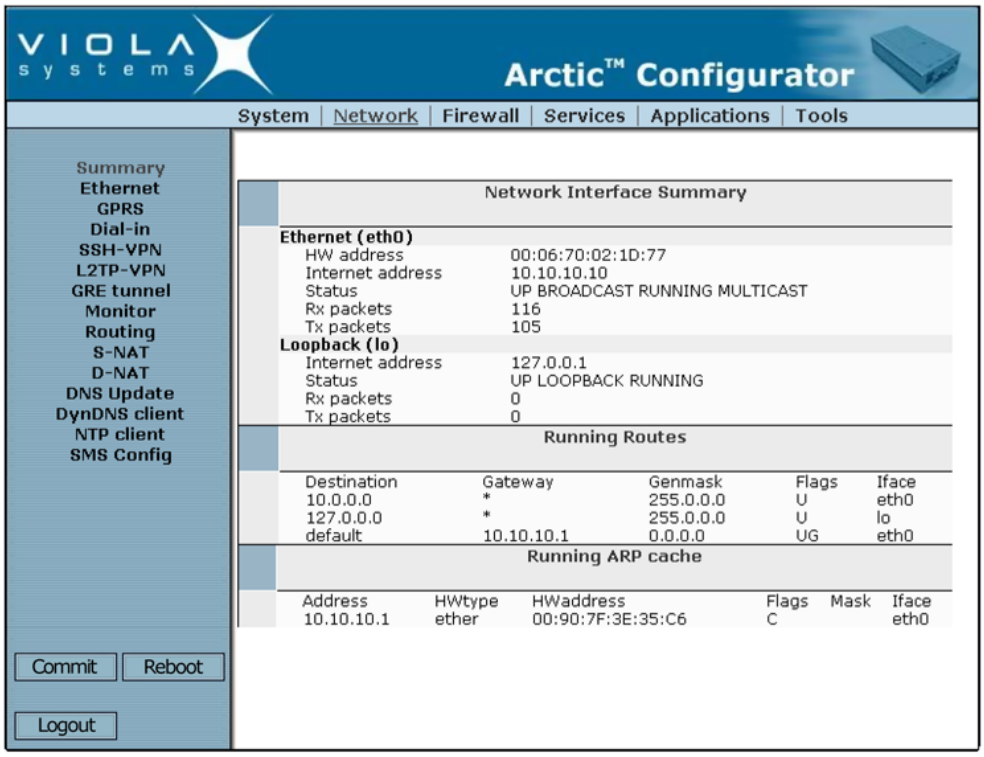
Environment – submenu contains information about the Arctic device memory usage, uptime and inside temperature.

Password – submenu contains password changing. The default password is blank. When changing the password for the first time, the same password has to be written in all three boxes.

6.2 Network Menu

Through the Network-menu you can access sub items to control the various network interface properties. The menu contains items for Ethernet, VPN and GPRS interfaces. Also Email, Proxy and firewall settings are located in this submenu. The **Network Interface Summary page** shows which interfaces are up and also routing information:

Figure 20. *Network Interface Summary*



6.2.1 Ethernet LAN

6.2.2 GPRS

GPRS settings include APN and other settings for GPRS network connectivity. More details of GPRS connectivity is in Chapter *GPRS*.

GPRS enabled – When set to yes, GPRS interface is automatically attached to GPRS network.

Access Point Name (GPRS) – GPRS Access Point (APN) name where the connection is made.

PIN code – SIM card pin code.

DNS servers – When set to “User defined”, DNS servers from Ethernet page are used. If the parameter is set to “From GPRS network” Arctic receives DNS server IPs automatically from GPRS network.

Led indication – In Data only mode, GPRS LED blinks green when transmitting data. In Informative mode, LED blinks also when connected to GPRS network without data transfer (GPRS context is active).

GPRS username – Username used for authentication if APN requires it.

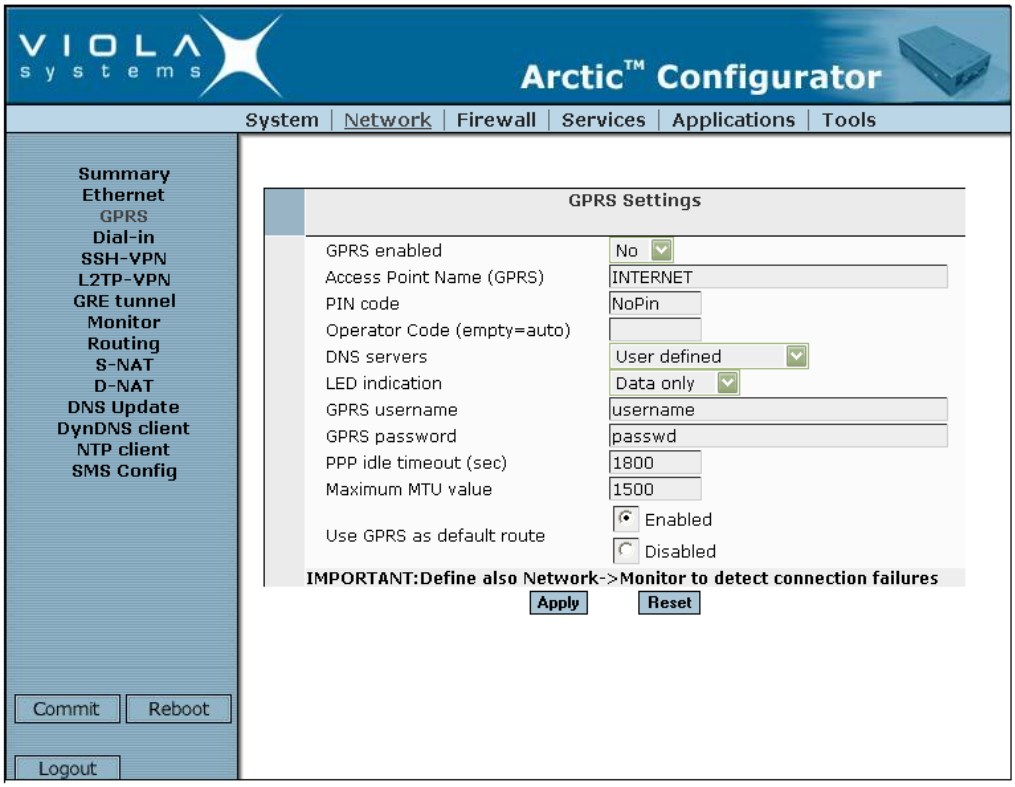
GPRS password – Password used for authentication if APN requires it.

PPP idle timeout – Maximum idle time for GPRS interface. If the GPRS interface has been idle (no traffic) for this period, the GPRS connection is restarted.

Maximum MTU value – MTU (Maximum transfer unit) for GPRS.

Use GPRS as default route – If enabled, GPRS is used as default route. Ethernet default gateway has to disabled (Parameter “Use Ethernet as default route” set to “No” in Network -> Ethernet).

Figure 21. *GPRS Settings*



6.2.3 Dial-in

Configuration for the Arctic PPP dial-in Interface.

Dial-in enabled – When enabled, PPP connections can be made to Arctic (GSM data).

Require authentication (PAP) – When set to *yes* password authentication is used for incoming data calls.

Required username – PAP username allowed login.

Required password – PAP password used for authentication.

Idle timeout – Idle time before PPP connection is terminated.

Local IP address – IP address used in PPP peer.

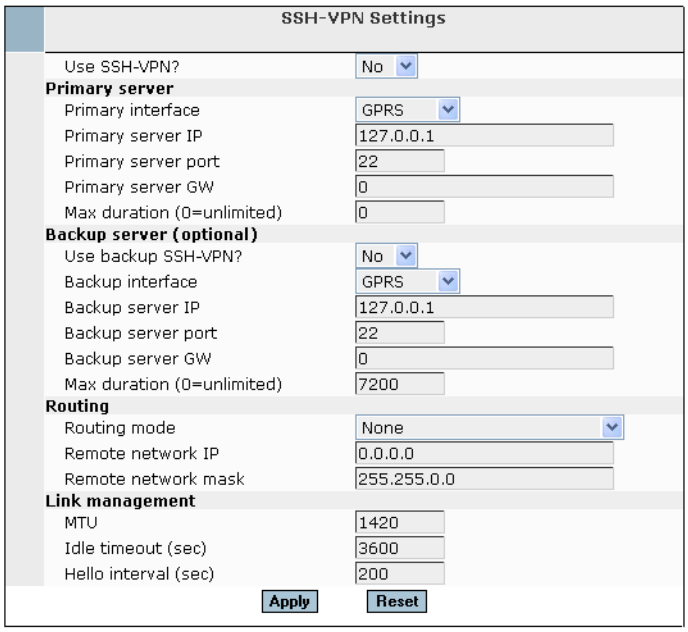
Peer's IP address – IP address used in PPP peer.

Maximum MTU value – MTU (Maximum transfer unit) for Dial-in connections.

6.2.4 SSH-VPN

Arctic has a VPN client that can be used with the Viola M2M Gateway. For VPN configuration, please refer to the Viola M2M Gateway User’s Manual.

Figure 22. *SSH-VPN Settings*



Primary server

Use SSH-VPN? – When set to "Yes" Arctic automatically establishes SSH-VPN connection to primary Viola M2M Gateway.

Primary interface – Interface used to reach the Viola M2M Gateway server.

Primary server IP – IP address of Viola M2M Gateway SSH-VPN server.

Primary server port – SSH-VPN TCP port on primary server (default 22).

Primary server GW – If other gateway than default route is needed to reach the Viola M2M Gateway.

Max duration (0=unlimited) – Maximum duration of the VPN connection. On primary server, should be set to zero. With backup server, after this timeout, the primary server is tried again.

Connection start timeout (sec) – Time to wait for the connection establishment.

Connection retry interval (sec) – How often retry the connection.

Connection retry mode – incremental increases the retry inteval on each connection attempt. Constant delay uses the same delay always.

Hello interval (sec) – Hello packet interval for the VPN. This can be used as a keepalive message on very critical links.

Hello failure limit – How many hello-packets can be lost before restarting the connection.

Backup server (optional)

Use backup SSH-VPN? – When set to “Yes”, Arctic will try to establish VPN connection to backup Viola M2M Gateway, if the primary cannot be reached.

Primary failure limit – How many times primary must not be reached, before changing to secondary.

Other parameters are same as in primary server. The duration of the connection can be set for example to 3600 seconds, so after one hour connection time to backup server the secondary is tried to be reached.

Routing

Routing mode – Routing mode has three modes:

1. "Tunnel the following network" - This adds the “Remote network IP” to be reached via the SSH-VPN. Parameters “Remote network IP” and “Remote network mask” must be set.
2. "Default route" -> VPN interface is used as default route.
3. “None” -> No routing is added when the VPN is established. The VPN peer IPs can be used for communications.

Remote network IP – Remote network IP behind the VPN (on Viola M2M Gateway side) what is needed to reached by Arctic.

Remote network mask – Netmask for remote network IP.

Link management

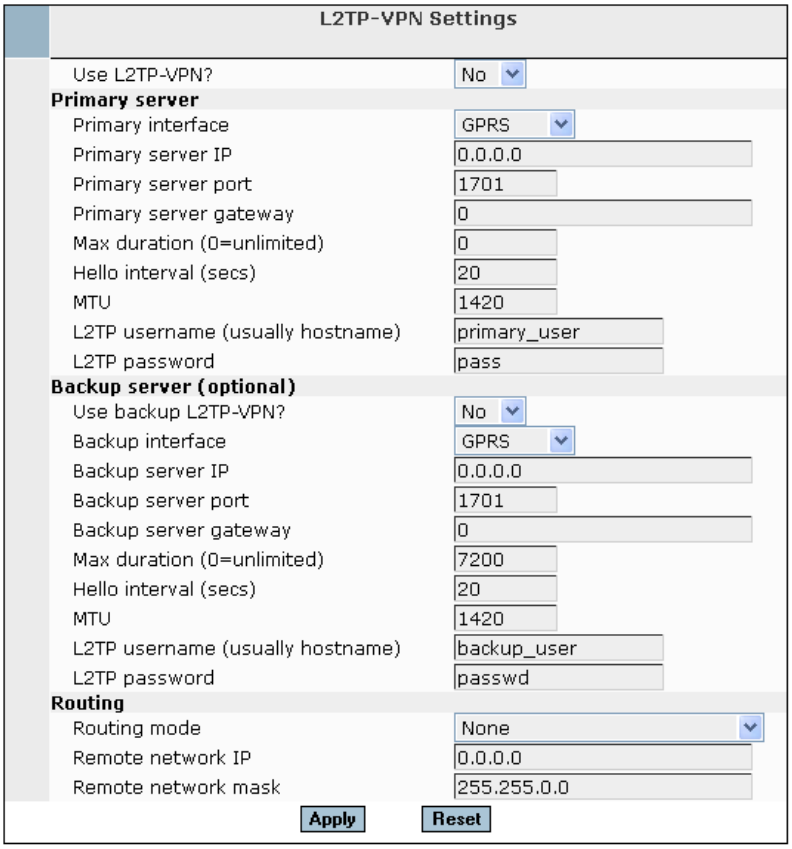
MTU – MTU for SSH-VPN interface.

Idle timeout (sec) – Idle timeout for SSH-VPN interface. If idle timeout is reached, the VPN connection is restarted.

6.2.5 L2TP-VPN

Arctic has a L2TP client that can be used with L2TP server.

Figure 23. *L2TP-VPN Settings*



Use L2TP-VPN? – When set to "Yes", Arctic established L2TP VPN connection with primary Viola M2M Gateway.

Primary server

Primary interface – Interface used to reach the Viola M2M Gateway server.

Primary server IP – IP address of Viola M2M Gateway L2TP server.

Primary server port – L2TP VPN server port (UDP, default 1701).

Primary server gateway – If other gateway than default route is needed to reach the Viola M2M Gateway

Max duration (0=unlimited) – Maximum duration of the VPN connection. On primary server, should be set to zero.

Hello interval (secs) – Hello interval for connection keepalive (default 20 seconds).

MTU – MTU for L2TP interface

L2TP username – (usually hostname) - Username for authentication.

L2TP password – L2TP password for authentication.

Backup server

If the primary server cannot be reached, the L2TP VPN connection is established with backup server.

Routing mode

It is used if routing is needed with L2TP interface. Configuration parameters are same as in SSH-VPN.

6.2.6 GRE

GRE tunnel enabled – When set to "Yes", Arctic establish automatically GRE connection

Interface – Interface used to reach the GRE server

GRE server IP – IP address of GRE server

Gw to GRE server* – (ethernet mode) If other gateway than default route is needed to reach the GRE server.

Local GRE interface IP – (usually eth0 IP) - Local IP used in GRE tunnel

Remote GRE interface IP* –Remote IP used in GRE tunnel

TTL value – Time-to-live value for the interface

Checksum* – checksum value.

Incoming key* – authentication key.

Outgoing key* – Outgoing key for the server

Routing

Routing mode – same as in SSH-VPN and L2TP

Remote network* – same as in SSH-VPN and L2TP

Remote network mask* – same as in SSH-VPN and L2TP

*These are optional, please refer to your GRE server documentation

6.2.7 Monitor

Monitor is used for GPRS and VPN connection checking. If connection to the selected IP address is lost, the connection is restarted. Monitor uses ICMP echo (ping) packets to check the connection. The monitor also keeps the connection alive, so that idle timeout do not drop the connections.

ICMP Echo sending – Selects if the monitor is enabled.

This should be always enabled to correct IP.

Interval (sec) – Determines how often the connection is checked by sending ICMP echo packets. The interval should be smaller than GPRS idle timeout (typically max. 2/3 of GPRS idle timeout) in order to have uninterrupted communication.

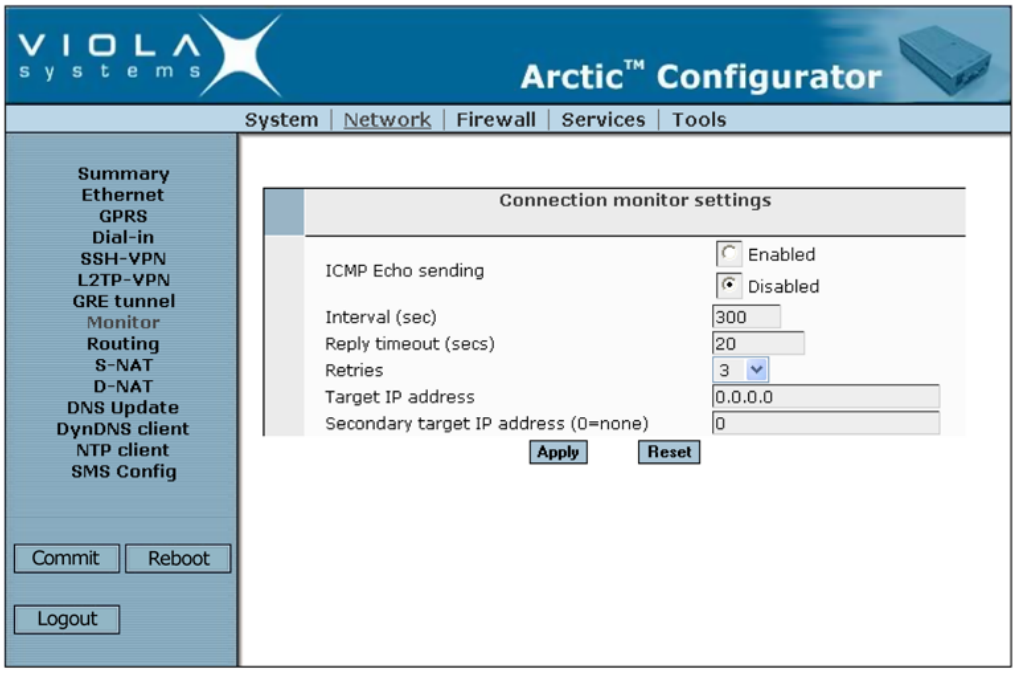
Reply timeout (secs) – The waiting time for reply packets.

Retries – The number of tries before connections are restarted.

Target IP address – The host IP address to which echo packets are sent to.

Secondary target IP address – The secondary host IP address to which ICMP echo packets are to be sent if the sending to primary target host IP address fails.

Figure 24. *Monitor Settings*



Note!

Monitor must be always enabled. When VPN is used, remote VPN peer IP (or other IP reached only via VPN) must be used for connection checking

6.2.8 Routing

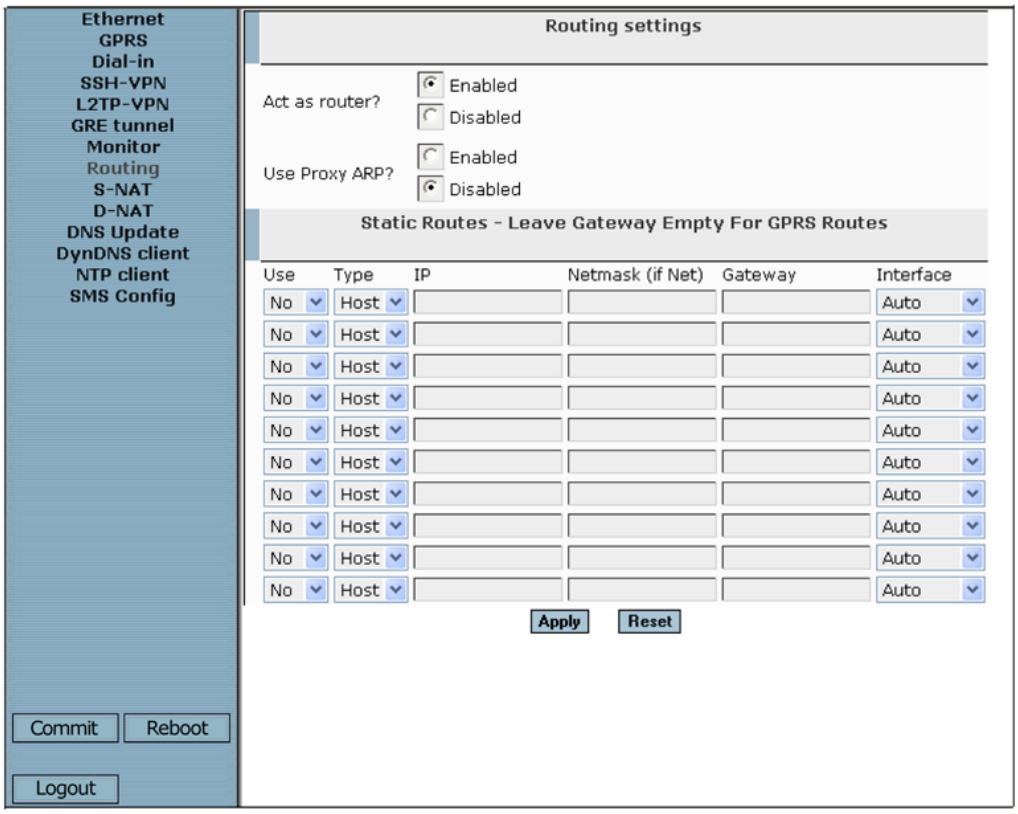
These parameters are used to configure routing settings

Act as router – Enables IP forwarding between interfaces.

Use Proxy ARP – Enables proxy ARP. It can be used with Viola M2M Gateway VPN.

Static routes can be added, if some hosts or networks require static routing settings.

Figure 25. *Routing Settings*



6.2.9 S-NAT

These parameters are used to configure S-NAT (source network address translation) settings. When enabled, private IP address used in local LAN is changed to GPRS interface IP address.

From IP – Only S-NAT connections from the defined IP address are accepted. If defined with wildcard (0/0), all IP addresses are handled the same way (only S-NAT connections are allowed).

6.2.10 D-NAT

These parameters are used to configure D-NAT (destination network address translation) settings. When enabled, packets coming to define GPRS interface port are forwarded to local IP address.

Source IP – D-NAT only connections coming from IP. Wildcard 0/0 means all IP addresses are D-NATted.

Protocol – Chooses which protocol is port forwarded. If “ANY” is chosen, other parametes are disregarded.

Dest.port – Chooses which GPRS interface is port forwarded to local Ethernet.

Redirect to IP – Chooses where port forwarding is done to.

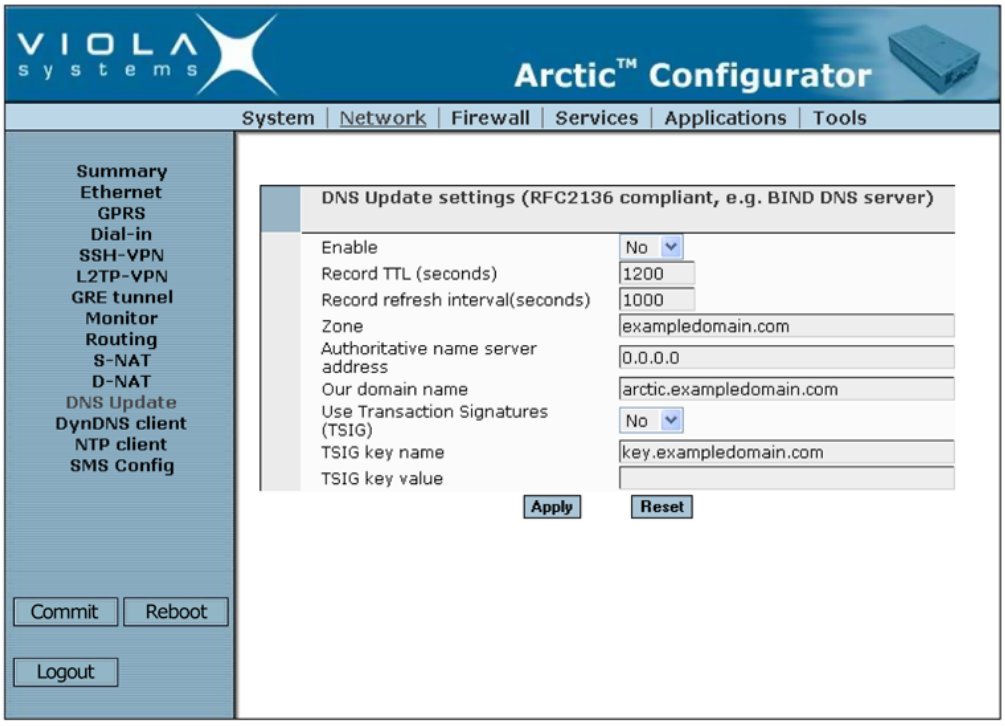
Redir. port – Chooses which port forwarding goes to.

6.2.11 DNS Update

These parameters are used to configure dynamic DNS. Arctic can report its dynamic IP address to a DNS server.

The DNS Update settings are RFC2136 compliant, for example BIND DNS server.

Figure 26. *DNS Update settings*



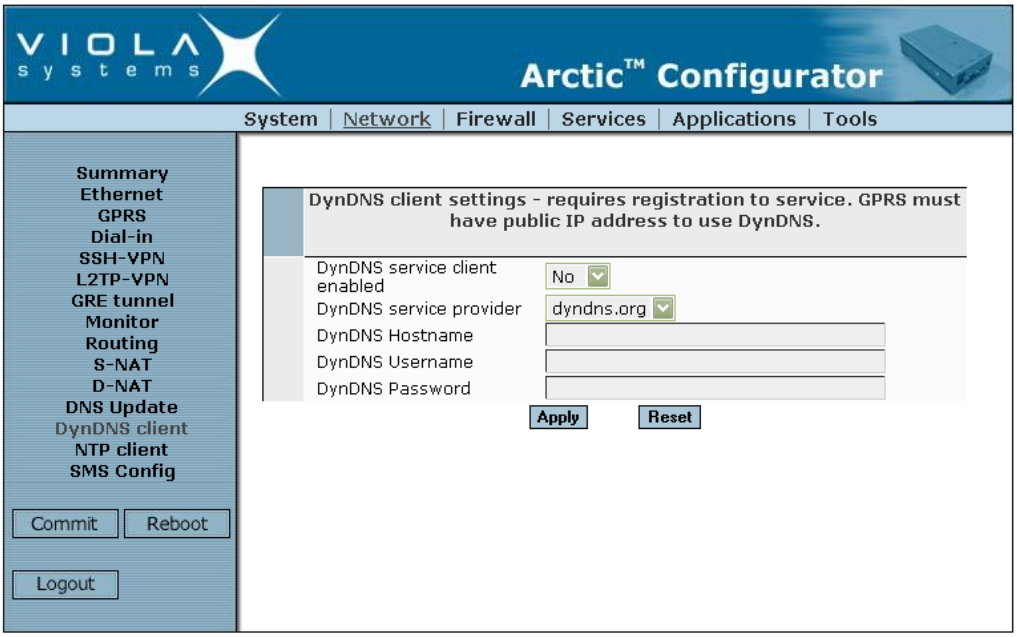
The server pointed by parameter “Authoritative names server” (eg. company’s own DNS server, for example ISC BIND) must be configured to accept incoming DNS update messages. TSIG keys can be used for better security in DNS updates.

6.2.12 DynDNS Client

This feature can be used with DynDNS service available at http://www.dyndns.org.

Note!
The public IP is required for GPRS and user account from the DynDNS service operator.

Figure 27. *DynDNS Client Settings*



DynDNS service client enabled – Disables or enables dynDNS DNS name update.

DynDNS service provider – Only dyndsn.org currently supported.

DynDNS Hostname – Service provider account hostname.

DynDNS Username – Service provider username.

DynDNS Password – service provider password.

6.2.13 NTP Client

This feature may be used to update the real time clock of Artic using NTP protocol.

NTP server – When set to "Yes", Arctic updates system clock from NTP server.

Query interval – How ofter NTP query is sent.

Minimum time difference (seconds) – Minimal time difference, when the clock is updated.

Maximum time difference – Maximum time difference between local system time and NTP time, when the clock is updated.

Time adjust mode –Adds or subsracts time from the received NTP value.

Time adjust value (minutes) – value to add or substract from NTP value.

6.2.14 SMS Config

This feature may be used to monitor the Artic status and to issue simple commands remotely via SMS messages. For detailed information, refer to “SMS Config Application Note”.

Enabled – Selects whether the SMS Config function is enabled or disabled.

Get commands

Access – Are get commands allowed for everybody, only for defined phone or are these disabled.

Allowed phone – Defined phone number for get commands.

Require password – Require system password for get commands.

Set commands

Access – Are set commands allowed for everybody, only for defined phone or are these disabled.

Allowed phone – Defined phone number for set commands.

Require password – Require system password for set commands.

Allow execute commands – Allow execute commands to be run on Arctic.

Other

Reply error to unknown commands – If set to "No", incorrect commands are silently disregarded. If set to "Yes", Arctic will send error SMS.

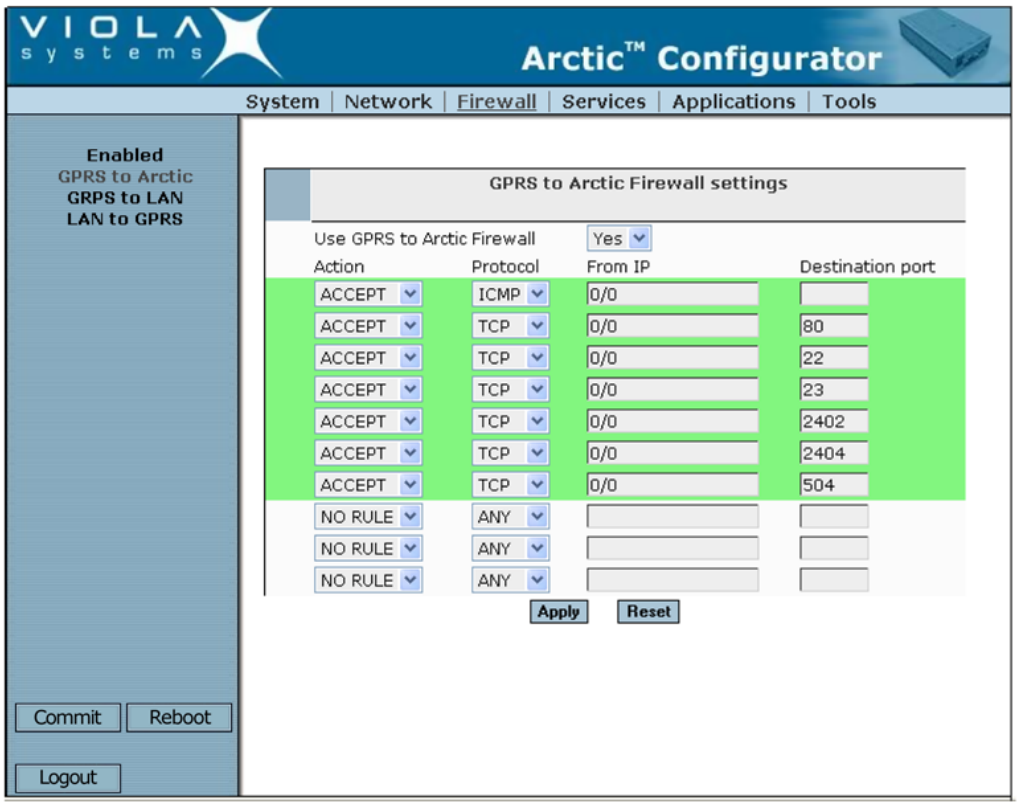
Reply error to unauthorized commands – If set to "No", unauthorized command are also silently disregarded. If set to "Yes", Arctic will send error SMS.

Factory reset command (8 chars min) – Command to issue device back to factory settings. This does not require system password. After issuing this SMS command, Arctic will have factory settings (eg. password is set back to factory default also).

6.3 Firewall Menu

Through the Firewall menu, you can configure built-in firewall of the Arctic. Firewall can be disabled or enabled and separate rules may be created for GPRS to Arctic, GRPS to LAN and LAN to GPRS.

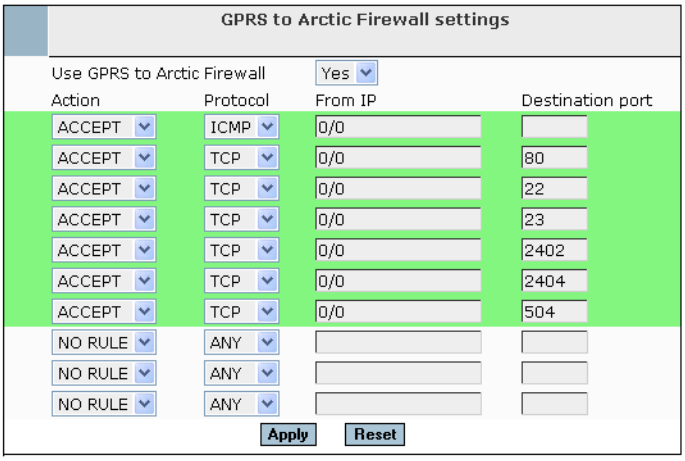
Figure 28. *GPRS to Arctic Firewall Settings*



The firewall rules are processed from top to bottom. If strict rules are wanted, last rule should be DROP.

The parameter “From IP” can be used for limiting access based on IP address. For example “192.168.100.0/24” would limit access only packets coming from 192.168.100.0 network.

Figure 29. *GPRS Settings*



These rules would allow incoming connection to GPRS interface: ICMP, web (TCP port 80) and telnet (TCP port 22) from any IP access.

6.4 Service Menu

6.4.1 Web Server

These settings enable or disable the web server functionality.

Web Server – Disables or enables the www server.

Web Configuration Access – Disables or enables web configuration access.

Note!
If you disable the web access settings, web configurator stops functioning and you will have to enable it via console if you should need to use it again later.

6.4.2 SSH

SSH server is available in Arctic for secure connections. Configuration file located at **/etc/sshd_config** may be edited manually.

SSH Server – Enables or disables the SSH server.

6.4.3 Telnet

Telnet server may be used to make terminal connections to the Arctic device shell. A more secure way of performing remote management is based on the SSH.

Telnet server – Enables or disables the telnet server.

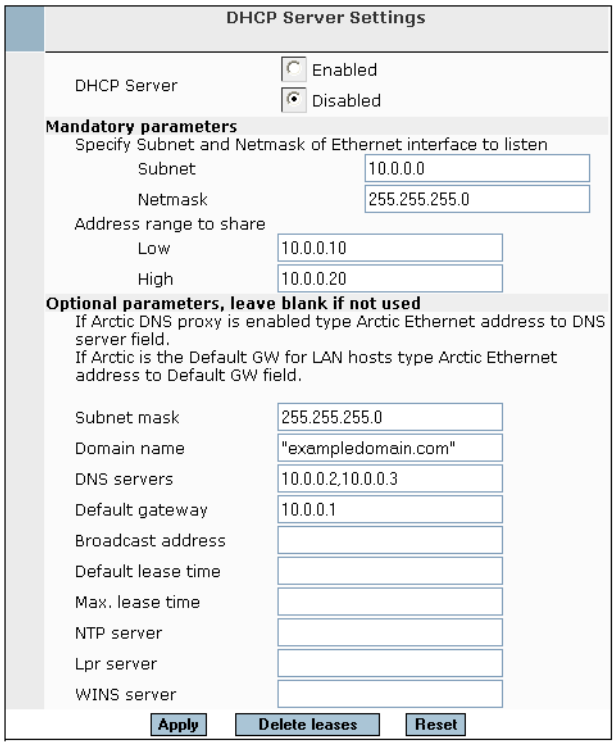
6.4.4 DHCP

DHCP server listens to broadcast DHCP queries and assigns IP address for host from the configured pool. If needed, Arctic can act as a DHCP server. This is suitable for small remote networks that have for example few laptops connected to the Arctic via an Ethernet hub or a switch.

DHCP Server

Enables or disables the DHCP server.

Figure 30. *DHCP Server Settings*



Note!
Configuring the DHCP server in an erroneous way may cause your network to function badly or may prevent functioning altogether. Consult your network administrator for necessary information **before** setting up the service.

DNS Proxy

With DNS proxy, computers connected to Arctic Ethernet interface can use Arctic as DNS server. Arctic will forward DNS queries to correct DSN server and local computers DNS setting are not needed to be changed. This can be used with GPRS settings (Network ->GPRS) parameter “DNS servers: From GPRS network”.

DNS Proxy/Forwarder –When set to ”Enabled” Arctic can be used as DNS server for local computers.

SNMP Agent

Arctic supports MIB-II SNMP Agent.

SNMP agent (SNMP Set/Get) – Set SNMP agent enabled or disabled.

Read only SNMP community – read only community string.

Read and write SNMP community – rw snmp community

Server port (standard=161) – Agent listen port (UDP)

Bind to interface – The interface is used as source address.

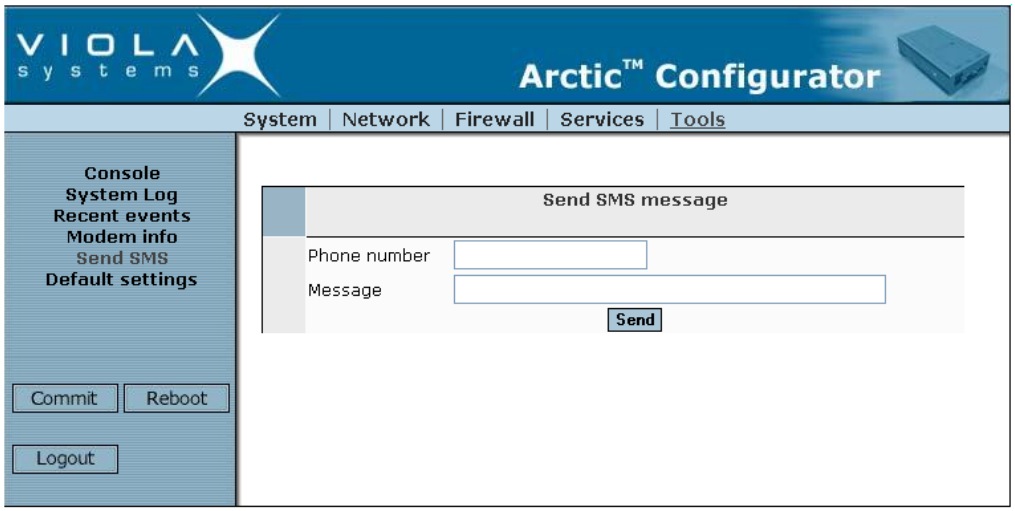
6.5 Application Menu

Application menu contains the serial device server application. With this application, serial devices can be connected to the Arctic Gateway and used over the TCP/IP network.

6.6 Tools Menu

The Tools menu provides the access to web based tools used for troubleshooting with the Arctic. It is possible to execute simple shell commands through the Web console. Also GPRS information can be obtained from “Modem Info” menu.

Figure 31. *Tools Menu*



Console

Console can be used for running command over the web interface. Example commands:

```
ping –c 10 172.30.30.1
firmware
```

System Log and Recent events

Arctic system log can be seen on system log and recent event. When support for device is need, full copy&paste from system log is needed.

Modem info

Arctic modem info show information about wireless connection status. Also the signal strength is shown here. This can be used for GPRS connection problems on site.

Send SMS

Arctic may be used for sending test SMS. This can be used for example checking the phone number of current SIM-card.

Default Settings

Arctic may be set to factory default settings from the Tools menu. This restores factory settings excluding network settings.

7 I/O Interface

This chapter describes the I/O hardware and related software (for interface extensions).

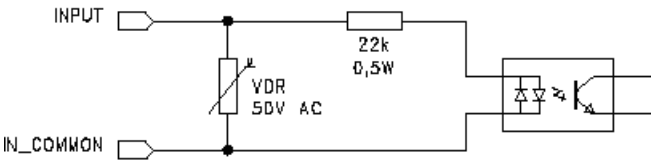
There are two types of I/O connector board:

IO-1	8 general purpose digital inputs, 2 digital outputs	Arctic RTU (2910 and 2920) product variants only.
IO-2	6 general purpose digital inputs, 4 digital outputs, 2 analog inputs	Arctic RTU (2930) product variant only.

7.1 Digital Input (IO-1)

For general purpose, digital I/O interfacing the Arctic includes eight digital inputs which all share a common reference pin. The inputs are optically isolated and work with voltage (bipolar) levels from 5 to 60 V and this range is guaranteed to be interpreted as a logical high state. Voltage levels less than 2 V are interpreted as a logical low state. The schematic of one digital input is shown in the figure below.

Figure 32. *Schematic Digital Input*



In the figure *INPUT* refers to one of the eight *Digital Input n -pins* and *IN_COMMON* refers to *Digital Input Common -pin* in the I/O connector's pin description is shown in the table below.

Table 4: IO-1 connector's pin description

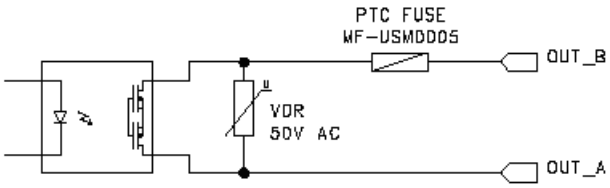
Pin #	Function
1	DC out
2	Digital input 1
3	Digital input 2
4	Digital input 3
5	Digital input 4
6	Digital input 5
7	Digital input 6
8	Digital input 7
9	Digital input 8
10	Digital input common
11	Digital output 1A
12	Digital output 1B

Pin #	Function
13	Digital output 2A
14	Digital output 2B
15	DC GND

7.2 Digital Output (IO-1)

The digital output of the Arctic is optically isolated and can be used for controlling low current external devices. The output is a CMOS relay which is protected by a PTC type fuse. The output is capable of handling a continuous current of 50 mA maximum at an ambient temperature of 20°C. In these conditions the output relay ON resistance together with the resistance of the fuse is typically about 50Ω which results in a 2.5 V loss across output pins with a full load current of 50 mA. The output schematic is shown in the figure below.

Figure 33. *Schematic Digital Output*



In the figure, *OUT_A* and *OUT_B* refer to *Digital Output nA* and *Digital Output nB* pins, respectively, in the I/O connector.

Note!

Absolute maximum voltage across digital output pins is 30 V. Voltage levels above this value may cause permanent damage to the PTC fuse.

7.3 DC Output

The input voltage to the DCIN connector is circulated back to the I/O connector of the Arctic. See the I/O connector's pin description table for more details. This DC output can be used, for example, together with digital outputs in order to simplify external circuitry and wiring.

7.4 IO-2 connector

The IO-2 connector and its inputs and outputs are described below.

Table 5: IO-2 connector's pin description

	Pin #	Description
AI01	1	Positive pin of analog input 1
	2	Negative pin of analog input 1
	3	Positive pin of analog input 2

	Pin #	Description
	4	Negative pin of analog input 2
	5-6	No connection
	7	DC supply output + input 5
	8	DC supply output - input 6
DI02	1-6	Digital inputs 1-6
	7	Common pin of the digital inputs
	8-11	Digital outputs 1-4
	12	Common pin of the digital outputs

7.4.1 Digital Input (IO-2)

For general purpose digital I/O interface of the Arctic includes six digital inputs which all share a common reference pin. The inputs are optically isolated and work with voltage (bipolar) levels from 6 to 60 V. This range is guaranteed to be interpreted as a logical high state. Voltage levels less than 1.65 V are interpreted as a logical low state.

7.4.2 Digital Output (IO-2)

Arctic has four isolated digital outputs with shared common pin. Digital outputs are polarity free.The digital output can be used for controlling low current external devices. The output is a CMOS relay which is protected by a PTC type fuse. The output is capable of handling a continuous current of 100 mA maximum at an ambient temperature of 20°C.

7.4.3 Analog Input (IO-2)

The analog input's characteristics are described in the tables.

Table 6: Analog input IO-2 characteristics

Parameter	Value	Note
Current measuring range	4-20 mA	Positive margin +15%
Input impedance	250 Ω	Current input
Maximum withstanding inputs	35 mA	Current input
ESD protection	82 V	Chip varistor protection
Isolation	100 V	

8 Modbus application settings

Note!
The information in this chapter applies only to Arctic RTU (2910) product variant.

8.1 Introduction

This Configuration guide is intended only for configuring Modbus on Viola Arctic device. It therefore presents only Modbus specific functionality.

The Modbus Gateway is an adapter application enabling conversions between Serial and Network Modbus protocols. The gateway can operate on two modes; either connecting serial Masters to Slaves behind the network or connecting network Master to Serial slaves.

The gateway offers following core properties:

- Supports Modbus RTU and Modbus ASCII serial protocols.
- Supports ModbusTCP, ModbusRTU over TCP, ModbusRTU over UDP, Modbus ASCII over TCP and Modbus ASCII over UDP network protocols.
- It can generate and filter out gateway exceptions.
- It can route traffic on network based on Modbus addressing enabling intelligent use of network resources.
- Makes automatic connection management.
- Enables multiple server sessions over network.
- Offers unlimited amount of Masters on serial or Network side.
- Offers 30 routes over network to slaves.

8.2 Parameters

The parameters are divided into two groups:

- Common parameters
- Routes

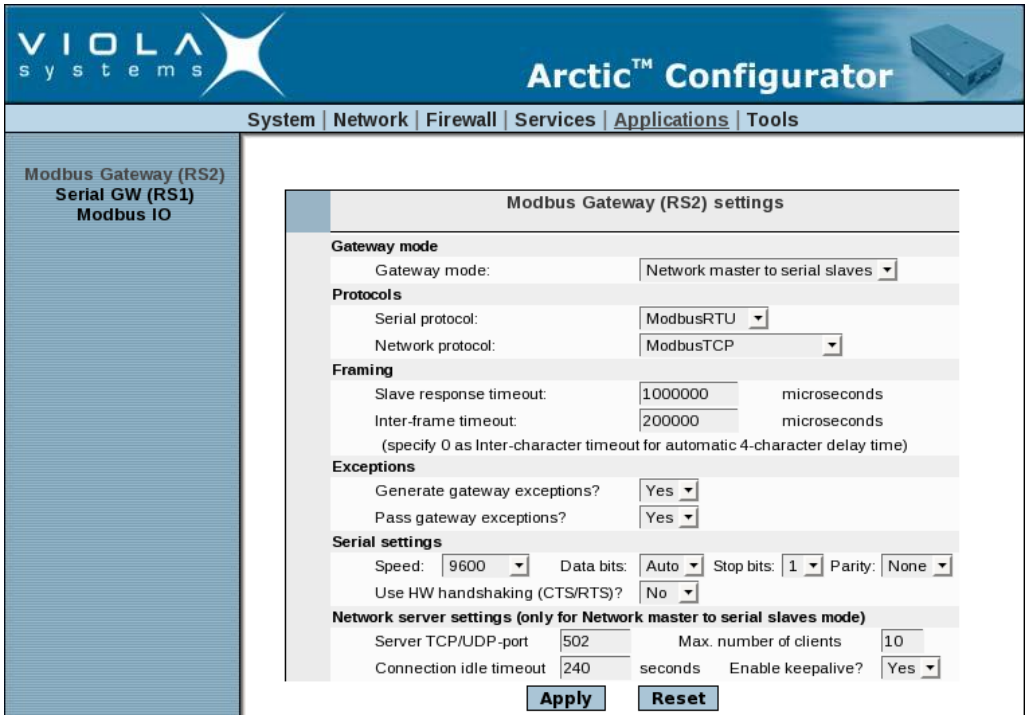
Common parameters define for e.g. the protocols used in serial and network communications, serial port settings and protocol specific timeouts. Route parameters are only required on Serial Master to Network Slaves mode defining the IP and Modbus addresses of slaves behind the network.

You can change the parameter values in **Applications > Modbus**.

8.2.1 Common parameters

The common parameters define general settings and settings for Network Master to Serial Slaves mode.

Figure 34. *Modbus application settings*


Arctic™ Configurator
System | Network | Firewall | Services | Applications | Tools
Modbus Gateway (RS2)
Serial GW (RS1)
Modbus IO
Modbus Gateway (RS2) settings
Gateway mode
Gateway mode: Network master to serial slaves
Protocols
Serial protocol: ModbusRTU
Network protocol: ModbusTCP
Framing
Slave response timeout: 1000000 microseconds
Inter-frame timeout: 200000 microseconds
(specify 0 as Inter-character timeout for automatic 4-character delay time)
Exceptions
Generate gateway exceptions? Yes
Pass gateway exceptions? Yes
Serial settings
Speed: 9600 Data bits: Auto Stop bits: 1 Parity: None
Use HW handshaking (CTS/RTS)? No
Network server settings (only for Network master to serial slaves mode)
Server TCP/UDP-port 502 Max. number of clients 10
Connection idle timeout 240 seconds Enable keepalive? Yes
Apply
Reset

General Settings

Gateway Status

Table 7: Gateway Status

Identifier	Gateway Status
Description	Tthe Modbus gateway functionality enabled for the serial port.
Values	Enabled – Modbus Gateway is enabled Disabled – Modbus Gateway is not enabled
Notes	Each serial port of Arctic has its own Modbus Gateway definitions.

Gateway Mode

Table 8: Gateway Mode

Identifier	Gateway Mode
Description	The slaves located on network or serial side.
Values	Network Master to Serial Slaves – Slaves are on serial side. Serial Master to Network Slaves – Slaves are on network side.
Notes	If slaves are on network side, the routes are also needed to be defined.

Protocols

Serial Protocol

Table 9: Serial Protocol

Identifier	Serial Protocol
Description	Defines the Modbus protocol used on serial communication.
Values	Modbus RTU – Serial devices use Modbus RTU protocol Modbus ASCII – Serial devices use Modbus ASCII protocol
Notes	Modbus RTU is more efficient and should be used whenever possible.

Network Protocol

Table 10: Network Protocol

Identifier	Network Protocol
Description	Defines the TCP/IP and Modbus protocol used on network communication.
Values	Modbus TCP – Modbus TCP protocol over TCP Modbus RTU over TCP – Modbus RTU protocol over TCP Modbus RTU over UDP – Modbus RTU protocol over UDP Modbus ASCII over TCP – Modbus ASCII protocol over TCP Modbus ASCII over UDP – Modbus ASCII protocol over UDP
Notes	If Viola Systems M2M Gateway is used to tunnel network traffic over SSH, use Modbus RTU over UDP when possible for efficient communication. The SSH tunnel already contains TCP properties like reliable message delivery.

Framing

Slave Response Timeout

Table 11: Slave Response Timeout

Identifier	Slave response timeout
Description	Defines the time in microseconds (10E-6 seconds) how long Arctic waits the response from Modbus slave. If the response is not received, Arctic can generate and return Modbus gateway exception.
Values	0 – 90 000 000 microseconds (0 – 90 seconds)
Notes	The reply timeout of Modbus Master must be greater than the Gateway (Arctic) timeout. Otherwise the flow of request-reply communication is violated. Arctic does not accept a new request before the reply from

Identifier	Slave response timeout
	slave is received or the reply timeout is elapsed. The delays in network communication can vary especially in wireless (e.g. GPRS/EDGE/ Mobitex) networks. When the slaves are located on network side, use e.g. PING to estimate the delay packets spend on network.

Inter-Frame Timeout

Table 12: Inter-Frame Timeout

Identifier	Inter-frame timeout
Description	Defines the idle time in microseconds (10E-6 seconds) that marks the end of Modbus frame in serial communication. If the value is zero, the Gateway uses standard 4 character time.
Values	0 … 2 000 000 microseconds (0 – 2 seconds)
Notes	Use as small value as possible to speed up communication and increase the value if problems arise. Some PC programs can insert unexpected delays between serial characters.

Exceptions

Generate Gateway Exceptions

Table 13: Generate Gateway Exceptions

Identifier	Generate Gateway exceptions
Description	Defines does the Gateway generate and return Modbus Gateway exception message to Master if no valid reply is not received from slave.
Values	Enabled – Generation of Gateway exceptions is enabled Disabled - Generation of Gateway exceptions is disabled
Notes	This functionality is useful for debugging. See also parameter “Pass Gateway exceptions”.

Pass Gateway Exceptions

Table 14: Pass Gateway Exceptions

Identifier	Pass Gateway exceptions
Description	Defines are the Gateway exception replies from slave side passed to master.
Values	Enabled – Gateway exception replies are passed to Master Enabled – Gateway exception replies are passed to Master
Notes	filtered away Notes

Serial Settings

Serial Port

Table 15: Serial Port

Identifier	Serial Port
Description	Defines the serial port that Gateway uses for Modbus serial communication.
Values	Port 1 – Serial port 1 (RS-232 console/application port) Port 2 – Serial port 2 (RS-232/422/485 application port)
Notes	If a single serial port or RS-422/485 is required, use Port 2. If Port 1 is used, the console switch of Arctic must be on Application position. DIP-switches below the DB-9 serial connector specify the RS-232/422/485 settings of Port 2.

Serial Speed

Table 16: Serial Speed

Header 1	Speed
Description	Defines the serial port speed for Modbus communication.
Values	300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps
Notes	Check the speeds supported by connected Modbus equipment. If special serial port speed is required, please contact Viola Systems.

Serial Data Bits

Table 17: Serial Data Bits

Identifier	Serial Data bits
Description	Defines the number of data bits used on Modbus serial communications.
Values	5, 6, 7, 8, Auto (8 for Modbus RTU, 7 for Modbus ASCII)
Notes	Check the data bits supported by connected Modbus equipment. Generally Modbus RTU communication uses 8 data bits and Modbus ASCII communication uses 7 data bits.

Serial Stop Bits

Table 18: Serial Stop Bits

Identifier	Serial Stop bits
Description	Defines the number of stop bits used on Modbus serial communications.
Values	1,2
Notes	

Serial Parity

Table 19: Serial Parity

Identifier	Serial Parity
Description	Defines the parity method used on Modbus serial communication
Values	None – no parity method used Even – even parity bit generated and inspected Odd – odd parity bits generated and inspected
Notes	

Serial Flow Control

Table 20: Serial Flow Control

Identifier	Serial Flow control
Description	Defines is the hardware (RTS/CTS) flow control used on Modbus serial communication
Values	Enabled – RTS/CTS flow control used Disabled – RTS/CTS flow control not used
Notes	Use of hardware flow control is suggested

Network Settings

Server TCP/UPD Port

Table 21: Server TCP/UPD Port

Identifier	Server TCP/UDP port
Description	Defines the TCP or UDP port that Masters can form connections to. Default Modbus TCP/IP communication port is 502.
Values	1 - 32500
Notes	If multiple Modbus Gateways are running on same device (for both serial ports) the TCP/UDP communication ports must not be same. Use e.g. ports 502 and 504. The network and Arctic firewalls must enable TCP or UDP communication for that port.

Maximum Number of Clients

Table 22: Maximum Number of Clients

Identifier	Maximum number of clients
Description	Defines how many network masters can be connected to Gateway simultaneously.
Values	0-20
Notes	Generally use value at least 2 when using TCP communication. Otherwise if the Gateway does not recognize partially closed

Identifier	Maximum number of clients
	connection, forming of new connections is not accepted by Gateway before “Connection idle timeout” is elapsed.

Connection Idle Timeout

Table 23: Connection Idle Timeout

Identifier	Connection idle timeout
Description	If the connected Master hasn’t sent valid Modbus packets during that timeout the connection is closed by Arctic and therefore the resources are available for new connections. This parameter is especially useful when the network connection is not reliable causing ’hanging’ or partially closed connections.
Values	0 – 32500 seconds
Notes	Set this value about two times the polling interval of master.

Enable Keepalive

Table 24: Enable Keepalive

Identifier	Enable keepalive
Description	Defines is the connection testing enabled for TCP network communication.
Values	Enabled – Testing the TCP connection with Master is enabled Disabled – Testing the TCP connection with Master is disabled
Notes	The testing is done by sending TCP keepalive packets on certain intervals.

8.2.2 Routes

When the Arctic Modbus Gateway is configured to Serial Master to Network Slaves mode the routes are needed to be defined for each connected Modbus slave. Gateway can route traffic based on Modbus addressing therefore enabling more efficient communication where each slave receives only data addressed to it.

Route in Use

Table 25: Route in Use

Identifier	Route in use
Description	Defines is this route entry used to decide to which IP address Modbus request is sent.
Values	Yes – Route information is used No – Route information is not used
Notes	If no route is found for Modbus request is it dropped and Gateway exception is generated if enabled.

Host

Table 26: Host

Identifier	Host
Description	Defines the IP address or Host name where packets are routed by that entry.
Values	IP address or Host name
Notes	If Host names are used the DNS server IP address is required to be defined on Arctic Network settings. The Network Protocol setting on “Common parameters” defines the network- and Modbus protocol used on network communication.

TCP or UDP Destination Port

Table 27: TCP or UDP Destination Port

Identifier	TCP or UDP destination port
Description	Defines the UDP or TCP destination port where this route entry sends Modbus requests.
Values	0 – 32500 (Modbus default is 502)
Notes	The port must be same as used on the network slave device or Gateway behind network.

Filter Slave Address

Table 28: Filter Slave Address

Identifier	Filter slave address
Description	Defines is the routing based on Modbus addresses used for that entry. If not enabled every Modbus request is routed to this entry. If enabled only Modbus requests having destination address matching the Address list of entry are routed.
Values	Yes – Route entry checks for Modbus destination address No – Route entry enables any Modbus destination address
Notes	It’s generally good to use Modbus address filtering avoiding unnecessary network traffic.

Address to Filter

Table 29: Address to Filter

Identifier	Address to filter
Description	Comma separated list of the Modbus addresses of slaves behind on this route entry (max. 20 pcs.).

Identifier	Address to filter
Values	Maximum 20 pcs. of comma (,) separated Modbus destination addresses.
Notes	The “Filter Slave address” parameter of Route entry needs to be enabled these addresses to take effect.

Connection Idle Timeout

Table 30: Connection Idle Timeout

Identifier	Connection idle timeout
Description	If there hasn’t been communication on this route during given amount of seconds the Gateway automatically closes the TCP connection to slave and therefore frees Slave’s communication resources. This is especially useful when multiple Masters access same Slave.
Values	0 – 32500 seconds
Notes	Set this parameter about two times the polling interval of Master.

Enable TCP Keepalive

Table 31: Enable TCP Keepalive

Identifier	Enable TCP keepalive
Description	Defines is the connection testing enabled for TCP network communication.
Values	Enabled – Testing the TCP connection with Slave is enabled Enabled – Testing the TCP connection with Slave is enabled
Notes	The testing is done by sending TCP keepalive packets on certain intervals.

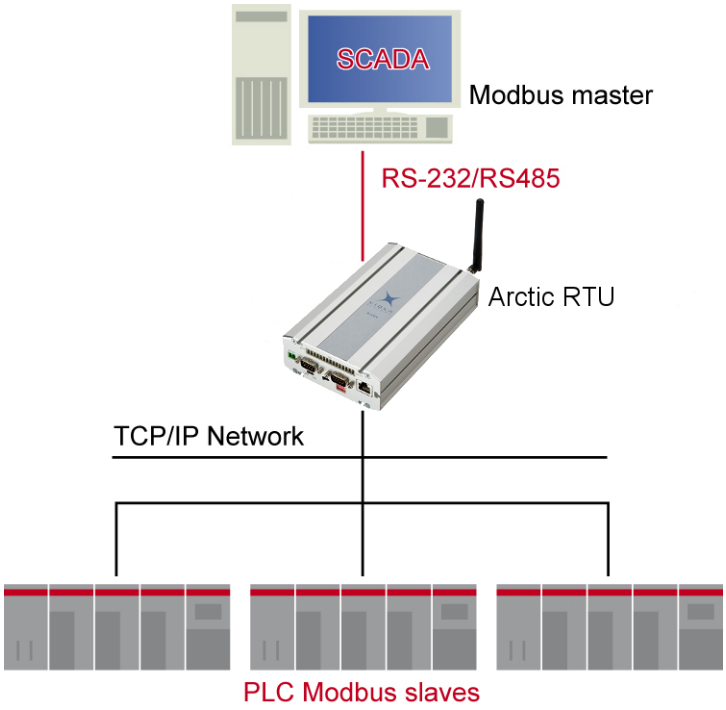
8.2.3 Saving Parameters

When the settings are complete, press the **Apply** button and permanently store the parameters by clicking on **Commit** button. Now reboot the Arctic by pressing **Reboot** button. The Arctic is now ready to deliver data from Network Masters to Serial Slaves.

8.3 Configuring Network Master to Serial Slaves Mode

When the PLC/RTU slaves supporting serial based Modbus communication are required to be controlled over TCP/IP networks the Gateway on slave side needs to be configured to Network Master-Serial Slaves mode.

Figure 35. *Arctic Modbus Gateway connecting serial slaves to network*



On that mode, the Arctic RTU acts like network server where Masters (clients) can connect (the default port being 502) and transmit Modbus requests. The RTU makes conversions between network and serial protocols. If the slave does not reply during defined timeout or if the reply is corrupted, the RTU sends “gateway exception message” back to Master if the exception generation is enabled. Otherwise, the reply is returned. Multiple masters can connect simultaneously to Gateway, which handles the multiplexing between masters.

Note!

Each Arctic RTU must have a fixed IP address in order the Master to know where to connect. Many client-use optimized networks (like public GPRS, xDSL) does not offer fixed IP addresses but allocate them dynamically. This situation can be solved by using Viola Systems M2M Gateway.

8.3.1 Settings – Common parameters

Only the common parameters are configured. The routes are unused on Network Master to Serial Slaves mode. The configuration menu is located on Applications -> Modbus GW menu of Arctic WEB configuration.

Figure 36. *Example of common parameters for Network Master to Serial Slaves mode*

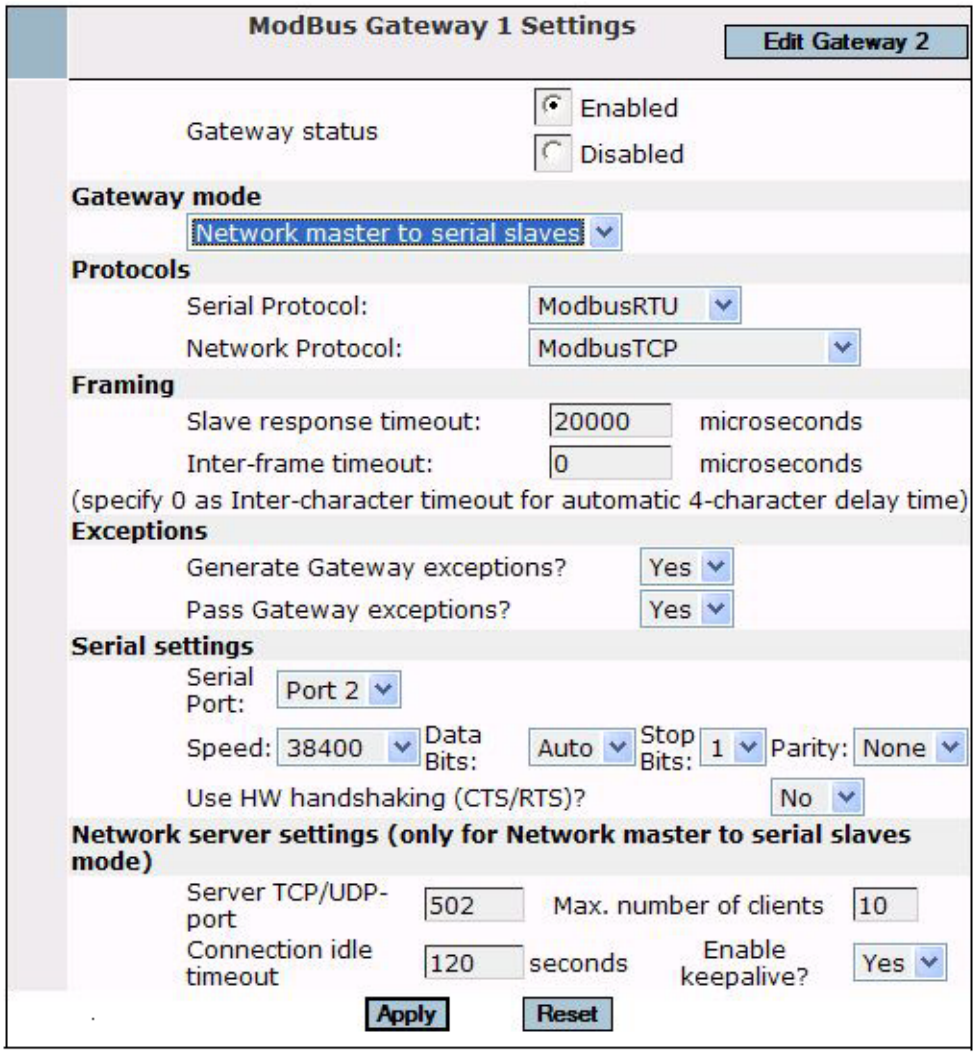


Table 32: Setting guideline for Network Master to Serial Slaves mode Parameter Value Note

Parameter	Value	Note
Gateway Status	Enabled	
Gateway Mode	Network Master to Serial Slaves	
Serial Protocol	Depends on connected Modbus slave	Prefer Modbus RTU when possible
Network Protocol	Depends on Master side	If Viola Systems M2M tunneling is used, prefer UDP based Modbus network messaging.
Slave response timeout	Depends on connected Modbus slave	Increase this value if problem is on serial communication.
Inter-frame timeout	Modbus RTU protocol has standard timeout of 4 character time. Use value 0 for default.	Increase this value if the problem is on serial communication.

Parameter	Value	Note
Generate Gateway exceptions	Enable or Disable	Enabling Gateway Exceptions can help system debugging and testing.
Pass Gateway exceptions	Enable or Disable	
Serial Port	Select Port 1 or Port 2	If single serial port or RS-422/485 functionality is required, use Port 2.
Serial Speed	Depends on connected Modbus slave.	
Serial Data Bits	Depends of connected Modbus slave. Use of “Auto” selects 8 data bits for Modbus RTU and 7 data bits for Modbus ASCII.	
Serial Stop Bits	Depends on connected Modbus slave.	
Serial Parity	Depends on connected Modbus slave. Select None, Even or Odd.	
Serial HW Handshaking	Enable if require by slave.	
Server TCP/ UDP Port	Default port for Modbus network communication is 502.	If multiple RTU applications are running on same Arctic, the ports must be different for each RTU application. Use e.g. ports 502 and 504.
Max. Number of clients	Normally use minimum value 2. If multiple Masters are allowed to connect, then increase the value.	If the network is wireless or unreliable, increase this value if there is a problem during the connection.
Connection idle timeout	Set about two times the polling interval of Master. If the polling interval is very long (over hour) use e.g. polling interval+200 seconds	
Enable keepalive	Enabled if the polling interval or idle timeout is very long.	

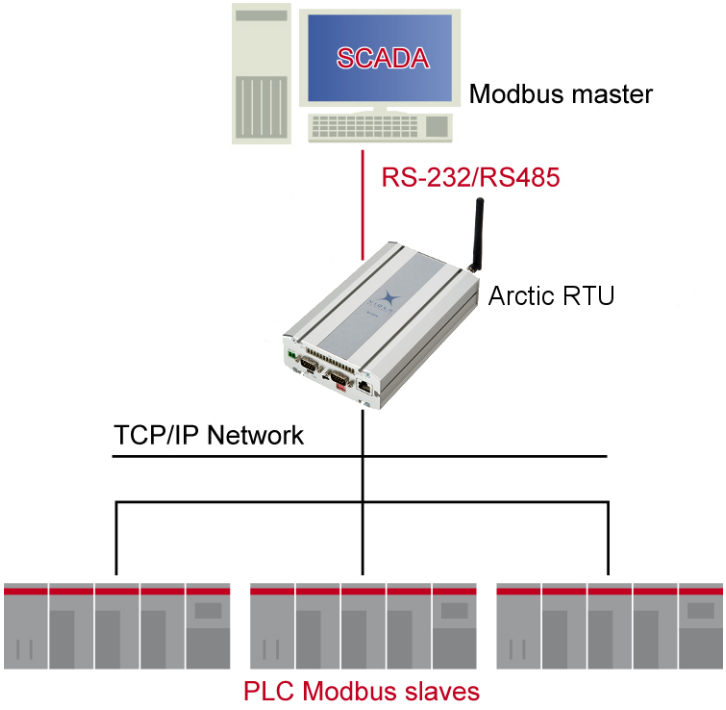
8.3.2 Saving Parameters

When the settings are complete, press the **Apply** button and permanently store the parameters by clicking on **Commit** button. Now reboot the Arctic by pressing **Reboot** button. The Arctic is now ready to deliver data from Network Masters to Serial Slaves.

8.4 Configuring Serial Master to Network Slaves Mode

When Modbus Master supporting serial based Modbus, communication needs to control slaves over TCP/IP network. The Gateway on Master side needs to be configured to Serial Master – Network Slaves mode.

Figure 37. *Arctic RTU connecting serial Master to network*



On that mode, Arctic RTU routes serial Modbus packets to network and performs conversions between serial and network protocols. The routing based on Modbus addressing allows intelligent use of network resources, which is especially useful for pay-per-use networks like GPRS.

The settings consist of two parts:

- Common settings
- Settings for each route

8.4.1 Settings – Common Parameters

The configuration menu is located on Applications -> Modbus GW menu of Arctic WEB configuration.

Figure 38. *Example of common parameters for Serial Master to Network Slaves mode*

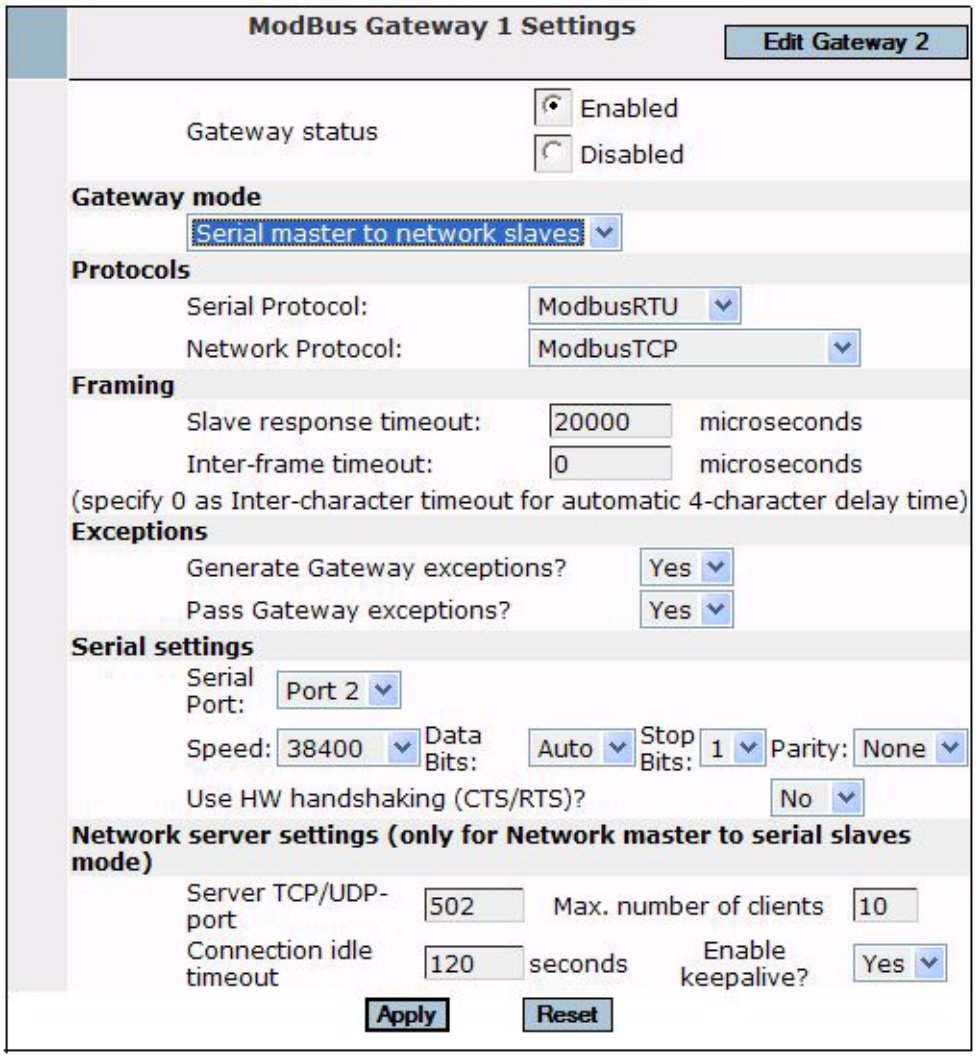


Table 33: Setting guideline for Network Master to Serial Slaves mode

Parameter	Value	Note
Gateway Status	Enabled	
Gateway Mode	Serial Master to Network Slaves	
Serial Protocol	Depends of connected Modbus Master	Prefer Modbus RTU when possible
Network Protocol	Depends of Slave devices	If Viola Systems M2M tunneling is used, prefer UDP based Modbus network messaging.
Slave response timeout	Depends of connected Modbus slave and delays of TCP/IP network.	Increase this value if problems on slave communication.
Inter-frame timeout	Modbus RTU protocol has standard timeout of 4 character time. Use value 0 for default	Increase this value if problems on serial communication

Parameter	Value	Note
Generate Gateway exceptions	Enable or Disable	Enabling Gateway Exceptions can help system debugging and testing
Pass Gateway exceptions	Enable or Disable	
Serial Port	Select Port 1 or Port 2	If single serial port or RS-422/485 functionality is required use Port 2
Serial Speed	Depends of connected Modbus Master	
Serial Data Bits	Depends of connected Modbus Master. Use of “Auto” selects 8 data bits for Modbus RTU and 7 data bits for Modbus ASCII.	
Serial Stop Bits	Depends of connected Modbus Master	
Serial Parity	Depends of connected Modbus Master. Select None, Even or Odd	
Serial HW Handshaking	Enable if require by Master	
Server TCP/ UDP Port	Default port for Modbus network communication is 502	Value is not used on Serial Master to Network Slaves mode.
Max. Number of clients	Normally use minimum value 2. If multiple Masters are allowed to connect increase the value.	Value is not used on Serial Master to Network Slaves mode.
Connection idle timeout	Set about two times the polling interval of Master. If the polling interval is very long (over hour) use e.g. polling interval+200 seconds	Value is not used on Serial Master to Network Slaves mode. Each route entry has it’s own idle timeout.
Enable keepalive	Enable if the polling interval or idle timeout is very long.	Value is not used on Serial Master to Network Slaves mode. Each route entry has it’s own keepalive setting.

Saving Common Parameters

Before proceeding to Route configuration, save the Common parameters by pressing the **Apply** button.

8.4.2 Settings – Routes

The route entries define how Modbus packets are routed on network from Serial Master to Network Slaves. Up to 30 routes can be specified each having up to 20 slaves. If the routing is based on Modbus addressing is not required or there are more than 20 slaves behind the route, the address filtering for that entry can be disabled.

Figure 39. *Route summary*

Routes to client/slaves (only for Serial master to network slaves mode)
ID Host Port Filter Slaves Idle timeout Keepalive
1 172.16.200.12 502 Yes 1,2 120 Yes
Edit
2 0.0.0.0 503 Yes 1 120 Yes
Edit
3 0.0.0.0 0 No 0 0 No
Edit

The route entry can be edited by pressing Edit button. The routes can also be disabled or enabled by pressing following buttons:

Disables the Route entry

Enables the Route Entry

The active routes do not have strikethrough line.

Pressing the Edit button opens following configuration screen:

Figure 40. *Route edit*

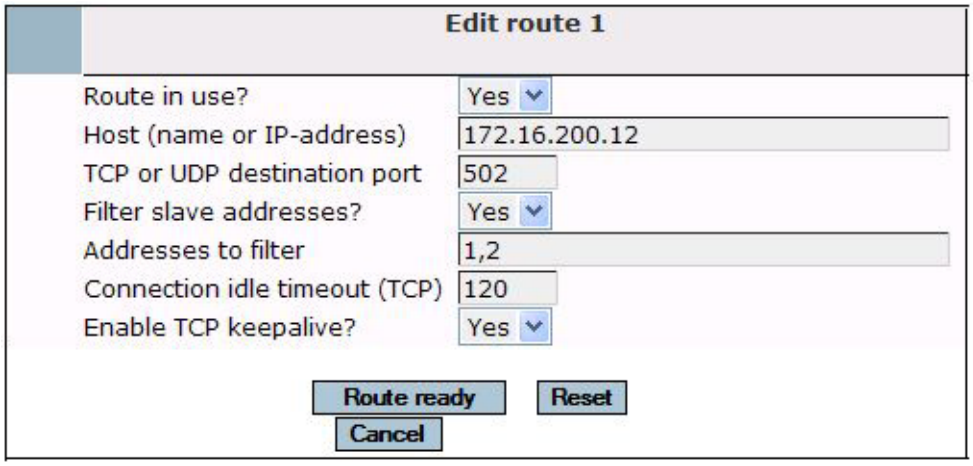


Table 34: Setting guidelines for Routes

Parameter	Value	Note
Route in use	Enable or Disable	Each IP address and TCP/UDP port of slaves needs to be defined on separate route entries.
Host	The IP address or Host name of slave or Gateway behind the route.	If Host names are used the DNS server IP address is required to be defined on Arctic Network settings. The Network Protocol setting on “Common parameters” defines the network- and Modbus protocol used on network communication.

Parameter	Value	Note
TCP or UDP destination port	The TCP or UDP port that slave or Gateway on slave side is listening.	Default Modbus port is 502.
Filter slave addresses	Defines is the routing based on Modbus addresses used for that entry. If not enabled, every Modbus request is routed to this entry. If enabled only Modbus requests having destination address matching the Address list of entry are routed.	It's generally good to use routing based on Modbus addressing in order to avoid unnecessary network traffic.
Address to filter	Comma separated list (max 20 pcs.) of Modbus slave addresses behind this route entry.	The "Filter Slave address" parameter of Route entry needs to be enabled these addresses to take effect.
Connection idle timeout (TCP)	Set about two times the polling interval of Master. If the polling interval is very long (over hour) use e.g. polling interval+200 seconds.	
Enable TCP keepalive	Enable if the polling interval or idle timeout is very long.	

Saving Routes

When the parameters are configured, press the Route Ready button and proceed to next route.

8.4.3 Making Settings Permanent

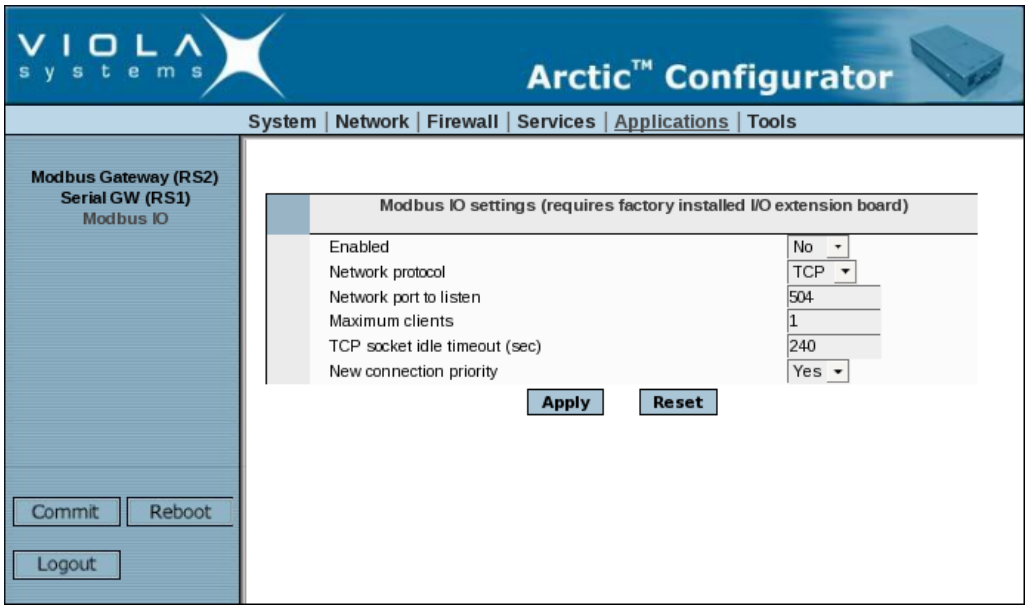
When all Routes and Common settings are configured permanently store the parameters by **Commit** button and reboot the Arctic Modbus Gateway. The Arctic is now ready to deliver data from serial Masters to network Slaves.

8.5 Modbus I/O settings

To change the Modbus I/O settings, go to **Applications > Modbus IO**. For more instructions on I/O port configuration, contact `support@violasystems.com`.

Modbus I/O settings for Arctic RTU (product variant 2910) (IO-1)

Figure 41. *Modbus I/O settings (2910)*



9 IEC-104 application settings

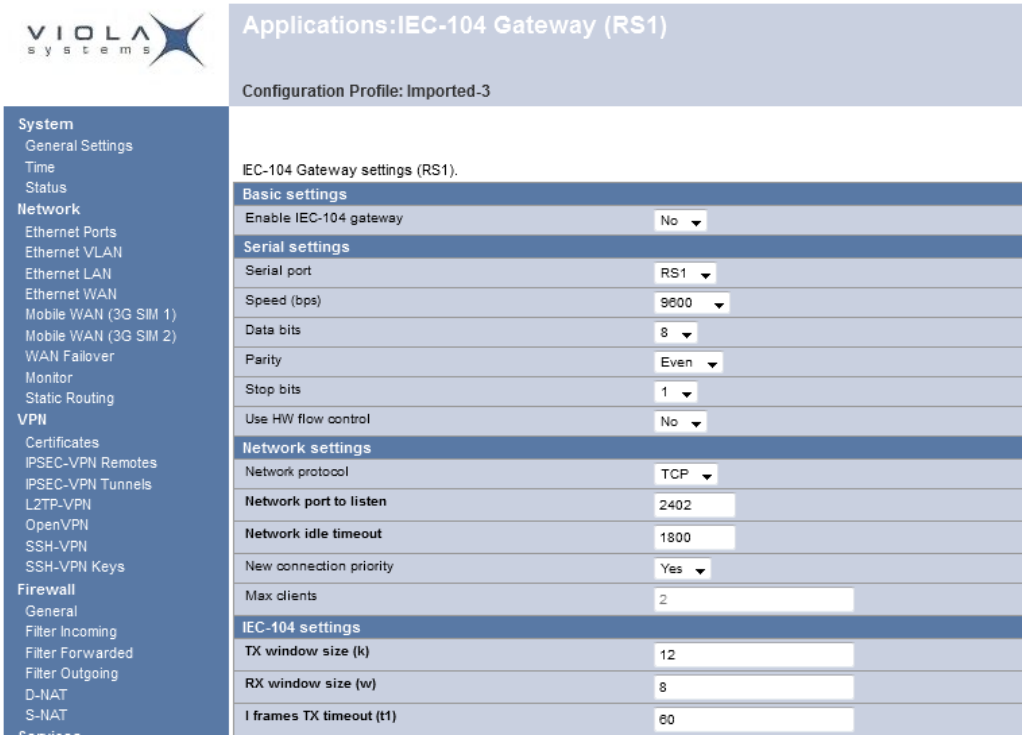
The IEC-104 and IEC-101 protocols share the same ASDU level messaging but differ on the link level. The IEC-104 is intended for packet-switched TCP/IP communication whereas the IEC-101 is intended for serial communication. By using the Arctic RTU, the IEC-101 slaves (e.g. RTUs) can be connected to a IEC-104 master (e.g. SCADA). The Arctic requests event from the IEC-101 slave locally and sends them to the IEC-104 master. This eliminates the need to continuously poll the data remotely and therefore reduces the communication costs on pay-per-use wireless network. This approach also eliminates the IEC-101 parameter adjutancy problems caused by variable round-trip delays on wireless networks and makes the information exchange faster and more reliable.

Note!

The information in this chapter applies only to Arctic RTU (2920 and 2930) product variants.

You can view and change the application settings in **Applications > IEC-104 (RSx)**.

Figure 42. *IEC-104 Application Settings*



9.1 General settings

IEC-104 gateway enabled

Enables or disables IEC-104 to IEC-101 gateway functionality.

Table 35: IEC-104 gateway enabled

IEC-104 gateway enabled	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	

9.2 Serial settings

The serial settings define the properties of physical serial communication between the Arctic and an IEC-101 slave. The selection between RS-232/422/485 is done with physical DIP switches located below the RS2 serial port.

Figure 43. *Serial Settings*

Speed (bps)

Table 36: IEC-101 serial communication speed (bps)

IEC-101 serial communication speed (bps)	
Type	Serial speed
Units	Bits per second
Value range	1200, 2400, 4800, 9600, 19200, 38400, 57600
Note	

Data bits

Table 37: Number of data bits used on IEC-101 serial communication

Number of data bits used on IEC-101 serial communication	
Type	Serial data bits
Units	Bits
Value range	5, 6, 7, 8
Note	

Parity

Table 38: Parity method used on IEC-101 serial communication

Parity method used on IEC-101 serial communication	
Type	Serial data parity
Units	Bits
Value range	None, Even, Odd
Note	

Stop bits

Table 39: Number of stop bits used on IEC-101 serial communication

Parity method used on IEC-101 serial communication	
Type	Serial data stop bits
Units	Bits
Value range	1, 2

Use HW flow control

Table 40: Number of stop bits used on IEC-101 serial communication

HW flow control mechanism (RTS/CTS) on IEC-101 serial communication	
Type	Boolean
Units	N/A
Value range	Yes, No
Note	The HW handshaking is available only on RS-232 mode.

9.3 Network settings

The Network settings define the general TCP/IP networking properties between the Arctic and the IEC-104 master.

Figure 44. *Network Settings*

Network protocol

Network protocol defines the network transmission layer protocol (either TCP or UDP) used on IEC-104 network communication. The IEC-104 standard protocol uses TCP but for reliable slow speed packet switched networks (e.g. Mobitex), the UDP protocol can be used to minimize the packets transmitted over network.

Table 41: Network protocol on IEC-104 communication

Network protocol on IEC-104 communication	
Type	Network transmission layer protocol
Units	N/A
Value range	UDP, TCP
Note	The IEC-104 standard specifies only TCP protocol.

Network port to listen

Table 42: TCP or UDP port to listen for incoming IEC-104 connections

TCP or UDP port to listen for incoming IEC-104 connections	
Type	Network port
Units	Port number
Value range	0 - 65000
Note	The IEC-104 standard specifies TCP port 2404.

Network idle timeout

It defines the idle timeout of the network connection in seconds. If there is no network data received during the specified interval, the connection is closed by Arctic. This parameter is required in order to detect partially closed connections and release the resources for new connections especially if the”New connection priority” parameter is disabled. Value 0 disables the network idle timeout detection.

Table 43: Network idle timeout for IEC-104 connections

Network idle timeout for IEC-104 connections	
Type	Timeout
Units	Seconds
Value range	0 – 65000
Note	The network idle timeout must be longer than IEC-104 link test interval (t3).

New connection priority

It defines the action when a new connection request arrives while a connection is already active. If the set value is”No”, the new connection is rejected. If the set value is”Yes”, the present connection is terminated and the new connection is accepted.

Table 44: New connection priority for IEC-104 connections

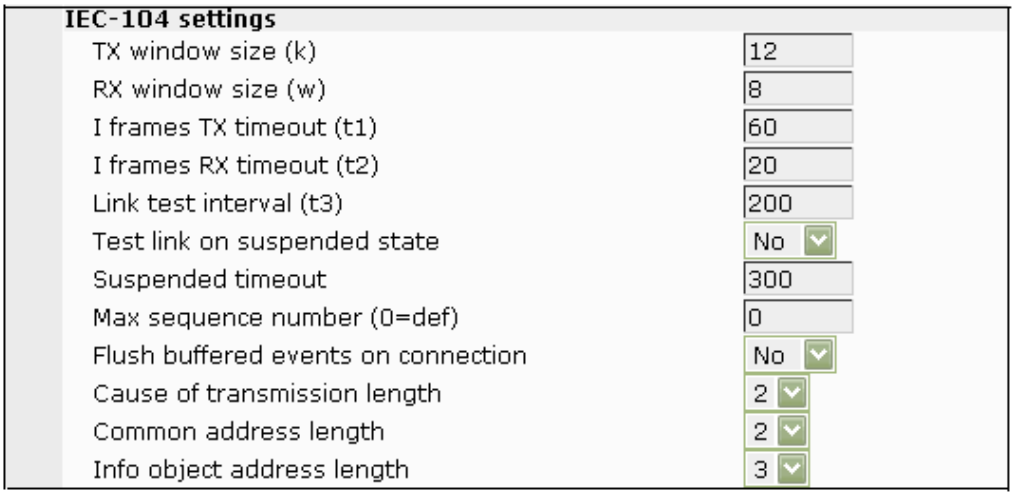
New connection priority for IEC-104 connections	
Type	Boolean
Units	N/A

New connection priority for IEC-104 connections	
Value range	No, Yes
Note	It is recommendable to set this value to “Yes” in normal configurations having only one IEC-104 master.

9.4 IEC-104 Settings

The IEC-104 settings define the properties of IEC-104 link layer and application layer parameters as described in the IEC 60870-5-104 standard. The IEC-104 communication is carried out between the Arctic and the IEC-104 master over the TCP/IP network.

Figure 45. *IEC-104 Settings*



TX window size (k)

TX window size defines the maximum number of I format APDUs the Arctic may send before requiring the IEC-104 master to acknowledge them. If there are *k* unacknowledged frames sent the Arctic will stop polling IEC-101 slave for events until acknowledgement is received.

Table 45: IEC-104 TX windows size (k)

IEC-104 TX windows size (k)	
Type	Window size
Units	Packets
Value range	1-20
Note	The *k* must be always less than the maximum sequence number defined below. The IEC-104 standard suggests *k* to be 12.

RX window size (w)

It defines the maximum number of I format APDUs the Arctic may receive before sending acknowledgement to the IEC-104 master.

Table 46: IEC-104 RX windows size (w)

IEC-104 RX windows size (w)	
Type	Window size
Units	Packets
Value range	1-20
Note	The *w* should not exceed two-thirds of TX window size *k*. The IEC-104 standard suggests *w* to be 8.

I frames TX timeout (t1)

It defines the timeout in seconds the Arctic waits for acknowledgement from IEC-104 master after sending last I format APDU or control frame (e.g. link test). If no acknowledgement is received during the defined time the Arctic will close the network connection and the IEC-101 link.

Table 47: IEC-104 I frames TX timeout (t1)

IEC-104 I frames TX timeout (t1)	
Type	Timeout
Units	Seconds
Value range	1-255
Note	The t1 must be longer than the network round-trip-time. The IEC-104 standard suggests 15 seconds.

I frames RX timeout (t2)

This defines the timeout in seconds from the last received I format APDU before sending acknowledgement.

Table 48: IEC-104 I frames RX timeout (t2)

IEC-104 I frames RX timeout (t2)	
Type	Timeout
Units	Seconds
Value range	1-255
Note	The t2 must be smaller than t1. The IEC-104 standard suggests 10 seconds.

Link test interval (t3)

This defines the interval in seconds how often the IEC-104 link is tested if there is no other activity.

Table 49: IEC-104 link test interval (t3)

IEC-104 link test interval (t3)	
Type	Timeout

IEC-104 link test interval (t3)	
Units	Seconds
Value range	1-65000
Note	Adjust this parameter according to the criticality of the link. The IEC-104 standard suggests 20 seconds but for pay-per-use GPRS connections the practical value may be substantially longer.

Suspended timeout

This defines the time in seconds how long a connected IEC-104 link can be in suspended state (STOPD) before the Arctic closes the connection.

Table 50: IEC-104 suspended timeout

IEC-104 suspended timeout	
Type	Timeout
Units	Seconds
Value range	1-65000
Note	Using this parameter increases the probability of detecting partially closed network connections especially in UDP mode.

Max sequence number

These are the maximum sequence number used in IEC-104 communication. The value zero selects the standard value 32767.

Table 51: IEC-104 suspended timeout

IEC-104 suspended timeout	
Type	Sequence number
Units	Packets
Value range	1-32767
Note	0 = 32767 as suggested by the IEC-104 standard.

Cause of transmission length (IEC-104)

It defines the length of IEC-104 Cause of transmission ASDU header field in bytes.

Table 52: IEC-104 ASDU cause of transmission length

IEC-104 ASDU cause of transmission length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-104 standard defines value 2.

Common address length (IEC-104)

This defines the length of IEC-104 Common address ASDU header field in bytes.

Table 53: IEC-104 ASDU common address length

IEC-104 ASDU common address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-104 standard defines value 2.

Info object address length (IEC-104)

This defines the length of IEC-104 Information object address ASDU header field in bytes.

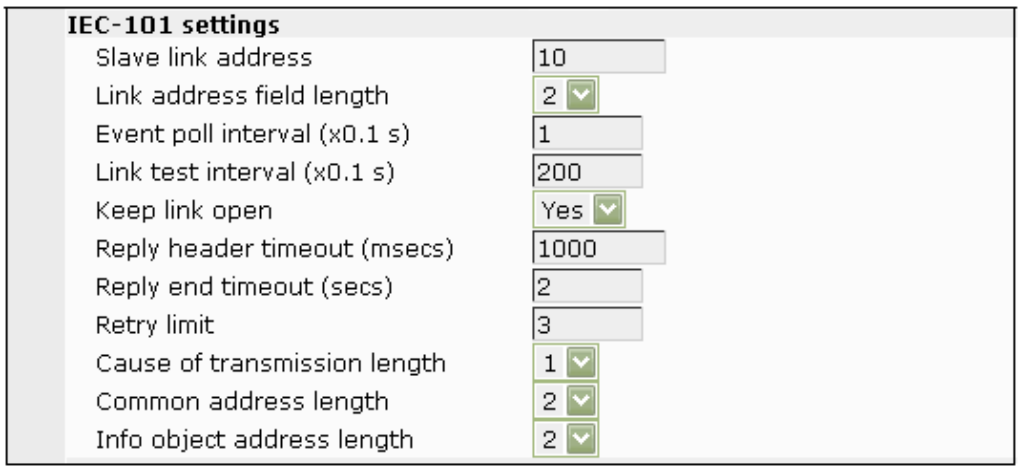
Table 54: IEC-104 ASDU information object address length

IEC-104 ASDU information object address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-104 standard defines value 3.

9.5 IEC-101 settings

The IEC-101 settings define the properties of IEC-101 link layer and application layer parameters as described in the IEC 60870-5-101 standard. The IEC-101 communication is carried out between the Arctic and a IEC-101 slave.

Figure 46. *IEC-101 Settings*



Slave link address (IEC-101)

Table 55: IEC-101 slave link address

IEC-101 slave link address	
Type	Link address
Units	N/A
Value range	1-65000
Note	The link-level address of IEC-101 slave.

Link address field length
Defines the length of the IEC-101 link-level address field in bytes.

Table 56: IEC-101 slave link address field length

IEC-101 slave link address field length	
Type	Field length
Units	Bytes
Value range	1, 2
Note	The link-level address of IEC-101 slave.

Event poll interval
It defines the IEC-101 event polling interval in 0.1 second increments (class 1 or 2 poll).

Table 57: IEC-101 event poll interval

IEC-101 event poll interval	
Type	Interval
Units	0.1 seconds
Value range	1-65000
Note	The events are polled only when the IEC-104 connection is active.

Link test interval
It defines the IEC-101 link test interval in 0.1 second increments. Link test is performed if there is no other activity.

Table 58: IEC-101 link test interval

IEC-101 link test interval	
Type	Interval
Units	0.1 seconds
Value range	1-65000
Note	The link test is performed if there is no other activity during defined interval.

Keep link open
Defines that the IEC-101 link is kept always open even when there is no active IEC-104 connection. If the functionality is enabled the Arctic sends link test frames and restarts the IEC-101 link if the test fails. The events are still not polled before the IEC-104 connection is active.

Table 59: IEC-101 keep link open

IEC-101 keep link open	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	Some IEC-101 slaves require the link to be continuously open in order to operate.

Reply header timeout
Defines the timeout Arctic waits the reply to start from IEC-101 slave after command or request.

Table 60: IEC-101 reply start timeout

IEC-101 reply start timeout	
Type	Timeout
Units	Milliseconds
Value range	1-65000
Note	

Reply end timeout
Defines the maximum duration of IEC-101 slave response.

Table 61: IEC-101 reply end timeout

IEC-101 reply end timeout	
Type	Timeout
Units	Seconds
Value range	1-65000
Note	

Retry limit
Defines the number of retries sent to a IEC-101 slave in case of no reply. If no reply is still received the Arctic closes the IEC-101 and IEC-104 connections.

Table 62: IEC-101 retry limit

IEC-101 retry limit	
Type	Retry limit

IEC-101 retry limit	
Units	Retries
Value range	0-65000
Note	

Cause of transmission length (IEC-101)
Defines the length of IEC-101 Cause of transmission ASDU header field in bytes.

Table 63: IEC-101 ASDU cause of transmission length

IEC-101 ASDU cause of transmission length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-101 standard defines value 1.

Common address length (IEC-101)
Defines the length of the IEC-101 Common address ASDU header field in bytes.

Table 64: IEC-101 ASDU common address length

IEC-101 ASDU common address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-101 standard defines value 2.

Info object address length (IEC-101)
Defines the length of IEC-101 Information object address ASDU header field in bytes.

Table 65: IEC-101 ASDU information object address length

IEC-101 ASDU information object address length	
Type	Field length
Units	Bytes
Value range	1-3
Note	The IEC-101 standard defines value 2.

9.6 ASDU Converter

The ASDU converter can be used to convert ASDU header field lengths between IEC-101 and IEC-104 protocols.

Figure 47. *ASDU Converter*

Use ASDU converter

This defines if the ASDU header level IEC-101 <-> IEC-104 conversion performed. If enabled the ASDU header field lengths are converted between IEC-104 and IEC-101. This parameter must be enabled if the ASDU header lengths differ between the IEC-104 and the IEC-101.

Table 66: Use ASDU converter

Use ASDU converter	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	The information on the field must fit in the shorter one of the two. It's not possible to convert e.g. value 12000 to a one byte field.

Use ASDU type replacer

The ASDU type replace function can be used to convert an ASDU type (Original type) to another (Applied type) type e.g. in cases when the IEC implementation differs between master and slaves.

Table 67: Use ASDU type replacer

Use ASDU type replacer	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	

Original type

The original ASDU type searched by ASDU type replacer.

Applied type

The new ASDU type is replaced by the original type.

9.7 Packet collector

The packet collector can be used to collect many IEC-101 messages/events to a single network packet instead of sending every message separately. This function is useful for slow packet switched communication network (e.g. Mobitex) for speeding up especially the general interrogation response.

Figure 48. *Packet Collector*

Use packet collector

Table 68: Use packet collector

Use packet collector	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	

Max bytes

Max bytes is defined as the maximum bytes trigger for packet collector. Before a new packet is inserted into the packet collector buffer the amount of bytes is checked. If the insertion of the new packet would cause the number of bytes in the packet collector to exceed MAX BYTES the old content is sent to the network before inserting the new one.

Table 69: Maximum collected bytes

Maximum collected bytes	
Type	Packet size
Units	Bytes
Value range	1-1500
Note	The value should be smaller than the MTU/MRU of network used.

Max time

Max time is deived as the maximum collect time trigger for packet collector in 0.1 secs increments for packet collector. If there has been data on packet collector over MAX TIME the data is sent to network.

Table 70: Maximum collected time

Maximum collected time	
Type	Timeout
Units	0.1 seconds
Value range	1-255
Note	The value must be smaller than t1.

Max packets

Max packets are defined as the maximum amount of IEC-101 packets stored into the packet collector before sending the data to the network.

Table 71: Maximum collected packets

Maximum collected packets	
Type	Packet count
Units	Packets
Value range	1-255
Note	

9.8 Other settings

Write syslog

It defines whether the error messages are stored to system log file or not.

Table 72: Write system log

Write system log	
Type	Boolean
Units	N/A
Value range	No, Yes
Note	The system log is available by using WEB UI.

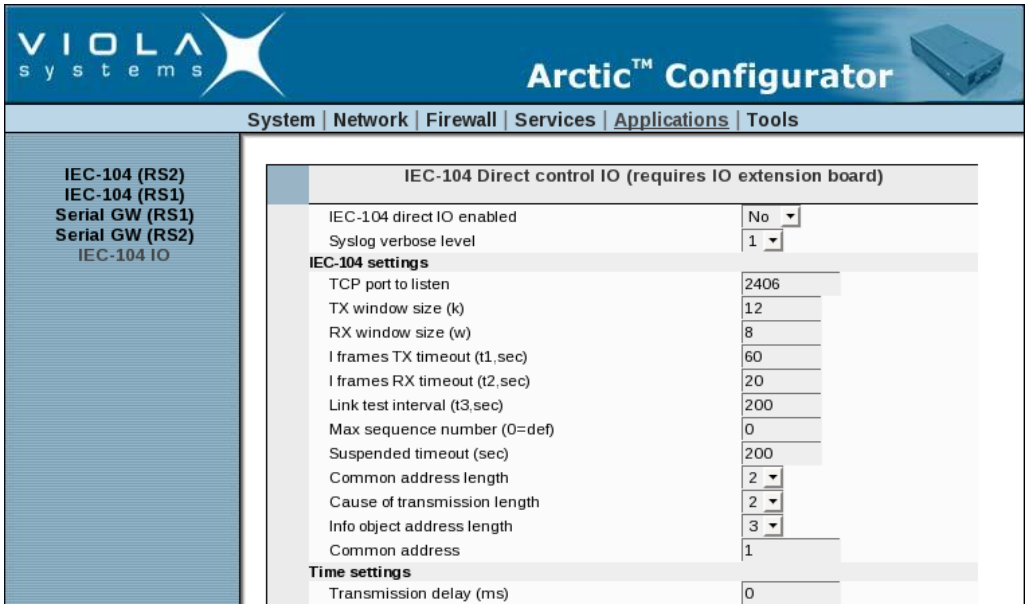
9.9 IEC-104 I/O settings

For more instructions on I/O port configuration, contact `support@violasystems.com`.

IEC-104 I/O settings for Arctic RTU (product variant 2920) (IO-1)

To change the IEC-104 I/O settings, go to **Applications > IEC-104 IO**.

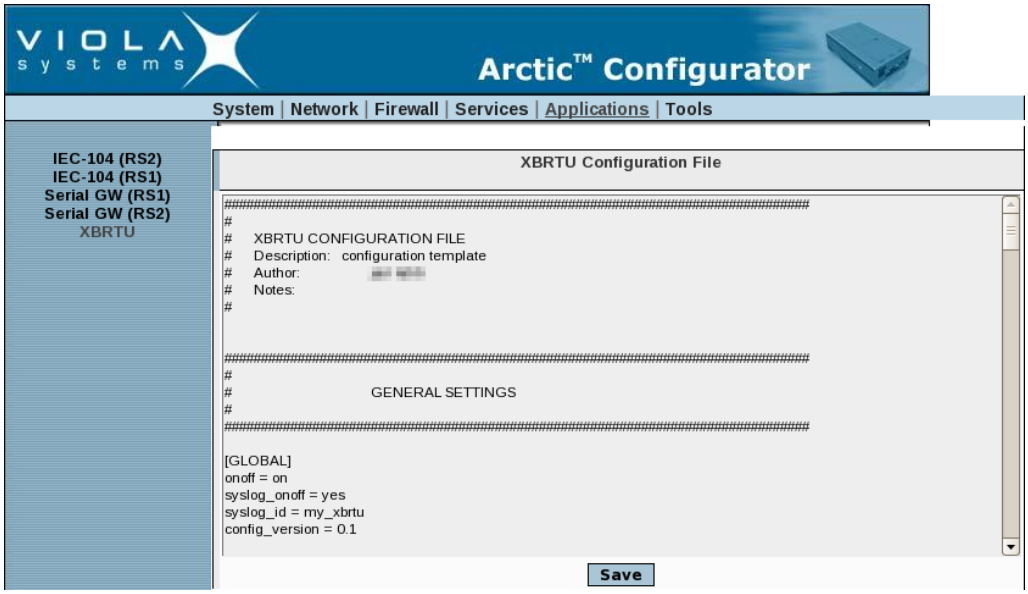
Figure 49. *IEC-104 I/O settings (2920)*



IEC-104 I/O settings for Arctic RTU (product variant 2930) (IO-2)

To change the IEC-104 I/O settings, go to **Applications > XBRTU**.

Figure 50. *IEC-104 I/O settings (2930)*



10 Troubleshooting

10.1 Common Problems

Problem #1

Q: Console does not receive characters.

A: Disable HW and SW handshaking from you terminal software (e.g. Hyperterm or Minicom).

Problem #2

Q: GPRS interface is up but no traffic flows through it.

A: Default gateway in Ethernet settings submenu has to be set as “0” and also default gateway has to be enabled from Network/GPRS menu when using GPRS interface as the default gateway.

Problem #3

Q: GPRS connection is not established.

A: Check that the SIM card has the correct PIN number settings and that it has not been locked after a wrong number was entered three times successively. PIN status can be checked from Tools/Modem Info menu.

Problem #4

Q: GPRS connection is ended after approximately two minutes.

A: You have enabled connection checking from Network/Monitor menu but not set the correct IP to GPRS “ICMP Echo settings”.

Specifications

Limited Warranty

Coverage

Viola Systems warrants this hardware product to be free from defects in materials and workmanship for the warranty period. This non-transferable, limited warranty is only for the first end-user purchaser. The warranty begins on the date of purchase and lasts for the period specified below:

Arctic RTU: one (1) year

Excluded Products and Problems

This warranty does not apply to: (a) Viola Systems software products; (b) expendable components such as cables and connectors; or (c) third party products, hardware or software, supplied with the warranted product. Viola Systems makes no warranty of any kind on such products which, if included, are provided "AS IS." Excluded is damage caused by accident, misuse, abuse, unusually heavy use, or external environmental causes.

Remedies

The sole and exclusive remedy for a covered defect is repair or replacement of the defective product, at Viola Systems' sole option and expense, and Viola Systems may use a new or refurbished parts or products to do so. If Viola Systems is unable to repair or replace a defective product, an alternate exclusive remedy shall be a refund of the original purchase price.

The above is Viola Systems' entire obligation to you under this warranty. IN NO EVENT SHALL VIOLA SYSTEMS BE LIABLE FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, USE, OR PROFITS EVEN IF VIOLA SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Viola Systems' liability exceed the original purchase price of the device server. Some states or countries do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply.

Obtaining Warranty Service

It must be notified to Viola Systems within the warranty period to receive warranty service. During the warranty period, Viola Systems will repair or replace, at its option, any defective products or parts at no additional charge, provided that the product is returned, shipping prepaid, to Viola Systems. All replaced parts and products become the property of Viola Systems. Before returning any product for repair, customers are required to contact the Viola Systems.

Technical Support

Contacting Technical Support

Phone: +358 20 1226 226

Fax: +358 20 1226 220

E-mail: support@violasystems.com

Internet: http://www.violasystems.com

Recording Arctic Information

Before contacting our Technical Support staff, please record (if possible) the following information about the Arctic product:

Product name:

_____

Serial no:

_____

Note the status of the Arctic in the space below before contacting technical support. Include information about error messages, diagnostic test results, and problems with specific applications.

_____

_____

_____